Anno 2 - N. 21
13 Marzo / 27 Marzo 2003

Boss: theguilty@hackerjournal.it

Editor: grAnd@hackerjournal.it,

Contributors: Bismark.it, CAT4R4TTA, DaMe`, Roberto "decOder" Enea, Lele - altos.tk, {RoSwElL}, Wolf Otakar.

DTP: Cesare Salgaro

Graphic designer: Dopla Graphic S.r.l. info@dopla.com

Publishing company
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, via Cavriana, 14
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

hack·er (hãk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

QUESTO È L'OPEN SOURCE, BABY...

Recentemente, in una mailing list mi è capitato di leggere un messaggio sull'open source. L'autore del messaggio si lamentava del fatto che una funzionalità di un software open source era stata "copiata" da un altro software analogo. La stranezza dell'affermazione dovrebbe saltare all'occhio, ma così non è per tutti.

Mi spiego. Uno dei principi più rivoluzionari del software libero è che gli autori mettono il codice (ma anche le idee) a disposizione della collettività, che può quindi prenderne dei pezzi e utilizzarli in altri modi. Il fatto quindi di poter "copiare" (come diceva l'autore del messaggio) è una caratteristica stessa dell'open source.

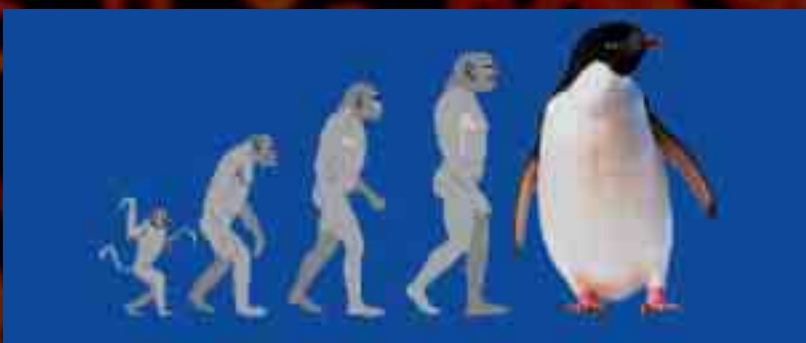
Nell'open source, più che copiare, si condivide il lavoro con gli sviluppatori di tutto il mondo, in modo che una buona idea possa propagarsi e migliorare in uno spirito di collaborazione, dove ognuno mette a disposizione le proprie capacità invece che nasconderle.

E, aggiungo, in questa copiatura trasversale di idee e di codice, accade che le idee più intelligenti vengono prese da chi scrive il codice migliore, e il codice ben fatto finisce per essere applicato a idee intelligenti, partorite da qualcun altro.

I prodotti intermedi (quelli che magari si basavano su una buona idea ma erano realizzati così così) si perdono per strada, ma consegnano i propri "geni" alla posterità. Si ha quindi una sorta di evoluzione darwiniana del software, nella quale la promiscuità genera (alla fine) sempre risultati migliori dei prodotti di partenza.

È buffo notare come anche tra chi usa e sostiene il software libero, ogni tanto ci sia qualche confusione. Il vecchio modo di vedere legato alla "proprietà intellettuale", in qualche modo, è troppo strettamente legato alla nostra cultura.

grand@hackerjournal.it

www.hackerjournal.it

Saremo di nuovo in edicola Giovedì 27 Marzo!

IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

UN RACCONTO OPEN SOURCE

Ci scrive Timekeeper: "Dopo tanto sentire e parlare di "Open source", mi è affiorata l'idea di "Open book", cioè dello sviluppo di un racconto a più mani, dove tutti possono partecipare allo sviluppo di un tema attraverso il proprio contributo di idee. [...] Mi piacerebbe sviluppare, nell'ottica sopra descritta, un soggetto in cui il protagonista o comunque il contesto sia legato al mondo dell'hacking. E chi meglio di voi e della comunità che vi segue potrebbe partecipare all'idea?"

Prima che vi tuffiate a partecipare, vi raccomando di leggere i termini della licenza del documento, che si rifà alla licenza per la documentazione libera GPL, ma riserva all'autore il diritto ad approvare le modifiche. Se per voi questi termini sono OK, allora fate un salto su http://werqw.supereva.it e… buon lavoro.

I NOSTRI/VOSTRI BANNER!

Nel momento in cui scriviamo, siamo arrivati a ben 38 banner realizzati da voi e pubblicati sul sito di HJ. Questi sono i più belli di questo giro, realizzati da 4ndr34, evaNder.sys e BigThistle.

Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: auto3no
pass: ma9lla

VENITECI A TROVARE!

Alcuni redattori di HJ parteciperanno come relatori a un seminario gratuito dal tema "La sicurezza in Mac OS X", organizzato da Mac@Work.

Il seminario si terrà sabato 29 marzo presso la sede di Mac@Work, in via Carducci angolo galleria Borella a Milano.

Per partecipare è necessario prenotarsi scrivendo all'indirizzo: corsi@macatwork.net

Su www.macatwork.net/store/formazione.html si possono anche trovare le date e gli argomenti di altri corsi e seminari gratuiti.

Dai bit alla carta

**ECCO ALCUNI DEI VOSTRI SITI.
Se volete comparire in questo spazio, scrivete a: redazione@hackerjournal.it**

www.hackmeetnaples.cjb.net

www.vincos.it/ictrlu.htm

www.jocker88.too.it

www.theblackzone.too.it

http://daemoncacum.cjb.net

mailto:
redazione@hackerjournal.it

MAC E NUMERI IP

Possiedo un iMac 450+. Volevo sapere se esiste un' utility in grado di dirmi il numero ip di chiunque (mac e pc) si connetta a me per esempio tramite un programma di messaggistica (MSNMessenger, icq ecc). Inoltre ho notato che molto difficile trovare dei numeri ip. Neanche cliccando sui contatori di shinystat si riesce. Potreste suggerirmi un modo per trovare liste di numeri ip?

fonzie

Su Mac OS 9 c'era l'ottimo IP Net Monitor (www.sustworks.com/site/prod_ipmonitor.html). In realtà c'è anche su Mac OS X, ma puoi farne a meno usando il comando netstat -a dal terminale oppure dal programma Utility Network, che trovi nella cartella Applicazioni/Utility.
Per quanto riguarda la tua seconda richiesta, scusa ma davvero non capisco cosa stai cercando. È come dire "dove posso trovare una lista di numeri di telefono"? Sono milioni, ma se non sai a chi corrispondono non servono a niente.

CONDIVISIONE DELLA CONNESSIONE

Vorrei avere delle informazioni a riguardo della linea ADSL. Io ho una flat di 256 kb/s e vorrei utilizzarla sia per il desktop che per il notebook. Ho contattato la ditta con cui ho l'abbonamento e mi ha riferito che dovrei cambiare abbonamento e usare un modem wireless. Vorrei chiedervi come potrei utilizzare questo modem che già ho senza cambiare abbonamento per sfruttare ambedue i pc?

Jean

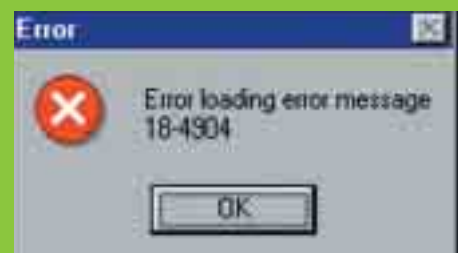
Ci sono due questioni, una tecnica e una legale. Cominciamo subito col dire che l'assistenza del tuo provider ha sicuramente sbagliato la risposta tecnica. Non è assolutamente necessario avere un "modem wireless" (definizione insesatta in sé) per condividere una connessione a Internet. Molto dipende dal tipo di modem che hai attualmente, ma in linea di massima occorre collegare i due PC con un cavo di rete, e usare un software di routing sul computer che è anche collegato al modem. Questo software è già presente in Windows nelle versioni dalla 98 SE in poi (Condivisione della Connessione Internet). Certo, un router wireless ti permetterebbe di andare in giro per casa con il tuo notebook navigando e scaricando la posta, ma a un costo di 250 euro circa (tra punto di accesso, il famigerato "modem wireless", e scheda wireless per il notebook). La seconda parte della risposta è relativa ai termini del tuo contratto. Molti contratti Adsl dedicati all'uso personale vietano l'utilizzo di più di un computer, anche se tecnicamente si può fare e ben difficilmente il tuo provider si accorgerà mai del secondo PC. Ora, visto che l'assitenza ha sbagliato la prima parte della domanda, ti consigliamo di spulciare il tuo contratto per vedere se per caso non ti ha dato una risposta sbagliata anche in questo caso.

ALLE PRIME ARMI

<P><STRONG><FONT style="BACK-GROUND-COLOR: yellow" face="Comic Sans MS"
color=red>Sono un hacker alle prime armi ma sto imporando molto in fretta.
Volevo sapere come funziona Try2Hack: come ottengo la password per passare il primo livello? Inoltre volevo sapere se una volta penetrato in una casella di posta altrui posso fare qualcosa di interessante oltre che scrivere e leggere le mail. Un'altra cosa: sono più volte che scarico Jonh the Ripper, Crackerjack e Unsecure (per Windows) ma nessuno di questi mi funziona.

Jack Fisher

*Scusa la franchezza, ma non sei *nemmeno* alle prime armi.*
Lezione n. 1: non scrivere mail in Html. È segno di maleducazione in Rete. Lezione n. 2: smembra, leggi, osserva, analizza. Guarda il codice sorgente della pagina. È da qui che devi partire, per questo giochino e per ogni altra cosa che tu voglia fare col computer.
Lezione n. 3: per scrivere mail con l'indirizzo di un altro non hai bisogno di entrare nella sua casella di posta. Ti basta cambiare i dati nel tuo client.
Lezione n. 4: entrare nella casella di posta di un altro significa compiere almeno due o tre reati.
E se la tua esperienza è quella dimostrata dalla prima domanda, ti beccheranno di sicuro. Lascia perdere.
Lezione n. 5: i "tool" non servono a niente se non capisci come funzionano.

☺ Tech Humor ☺

POSSIBILI ERRORI

- **Libreria mancante. Guardare in biblioteca**
- **Trovato terrorista. Spostarlo in cgi-bin-Laden?**
- **Attenzione, Apple ha rilevato un worm!**
- **Backdoor rigirata! Attenzione alla frontdoor**
- **Trovato Salam.sys, Panin.dll, Maiones.dat: è pronto il buffer!**
- **Errore in mIRC. Provare in gIANN?**
- **Errore terrificante: che hai fatto?!**
- **Erore inteno al Uindos! Zi è rolto ik corrreturu orpotrafico!**

(Grande Tommy)

www.hackerjournal.it

COSA SI RISCHIA?

Se una persona viene denunciata per aver usato una casella di posta elettronica di qualcun altro cambiando o usando la sua password cosa rischia? Come fanno a scoprire chi è stato ad appropriarsi della casella ? Un Minorenne rischia qualcosa?

<G!?X>

☺ Tech Humor ☺

A occhio, una pena fino a tre anni per l'intrusione in un sistema informatico (art. 615 ter del Codice Penale) e un anno per l'appropriazione di corrispondenza altrui (Art 616). Per scoprire chi è stato, le Forze dell'Ordine richiedono al provider il listato delle connessioni avvenute alla casella di posta; individuato l'indirizzo IP dell'intruso, lo incrociano con il log delle connessioni del provider di accesso, e rilevano l'account a cui corrisponde e il numero di telefono del chiamante. Se questo è stato nascosto, fanno un ulteriore incrocio coi log di Telecom o del gestore telefonico. Un minorenne che commetta un reato viene processato dal Tribunale dei Minori, che ha pene e regole diverse, ma in ogni caso non la passa liscia.

POSTA BUCA FIREWALL

Frequento un'università di agraria e la rete dei PC è protetta da un firewall (non so quale) che mi nega l'accesso al mio account di posta su libero. Ho provato anche con telnet (non sono molto pratico…) e tutte le volte che provo a connettermi con quel programma, mi da connessione fallita. Vorrei sapere se potete aiutarmi in qualche modo o ad aggirare questo firewall o a utilizzare Internet; non penso sia contro la legge leggere la propria posta! Voi direte "perchè non provi a cambiare account di posta?". È una questione di principio per prima cosa, e secondariamente ho veramente troppe persone a cui dovrei dare il mio indirizzo di posta elettronica…

Alberto

☺ Tech Humor ☺

New hardware-device from Microsoft

Puoi provare a usare un sito che ti permetta di leggere la mail da caselle POP3 esterne, come il servizio Mail di Yahoo! (puoi impostare fino a 3 caselle esterne, e leggere la posta attraverso il Web). Se non ti va di iscriverti a un servizio, puoi usare Mail2Web www.mail2web.com, che fa le stesse cose ma senza bisogno di registrazione (ogni volta però dovrai inserire indirizzo del mail server, nome utente e password.

SOFTWARE PER STEGANOGRAFIA

Fantastika redazione di HJ, ho 12 anni e mi ha interessato molto la steganografia:potete indikarmi dove trovare un programma in grado di kodifikare i testi invece di dovermalo kreare???
Grazie e continuate così xkè siete i migliori

kaz182

*Voilà:
www.topology.org/soft/crypto.html
www.cl.cam.ac.uk/~fapp2/steganography/stego_soft.html
Sono tutte raccolte di svariati programmi.*

...DICO LA MIA

Quante menate. L'hacker è un tizio buono il craker no, L'hacker è un tecnico che hackera senza fare danni, tutti gli altri sono vandali. Lui vuole solo capire e conoscere i sistemi altrui. Ha qualcosa di logico tutto ciò? Forse lui lascia l'auto aperta o il suo appartamento con la porta spalancata perchè altri possano studiare i suoi allarmi o altro?
E ancora, sicurezza sicurezza sicurezza, cassaforti, password, steganografia, dati al sicuro. Ma da chi? Io non sono un industriale, non sono un politico non un trafficante né un delinquente e la maggioranza della popolazione è così: con una busta paga, trattenute automatiche e una privacy che non esiste. Ci contano anche i peli del c***. Forse i vostri articoli sono propio indirizzati a questi personaggi ai quali occorre maggiore sicurezza x nascondere i loro brogli. A quelli come me nella malaugurata ipotesi c'è il Signor FORMAT.
Condannate chi attacca siti e multinazionali balorde, mentre io non sò far altro che compiacermene.

Ganiva

E adesso noi lasciamo che gli altri lettori dicano la loro. Siete d'accordo oppure no? Volete rispondere o commentare? Mandateci le risposte a redazione@hackerjournal.it

HOT!

LA ZETA JONES È UN VIRUS

Non ci riferiamo alla procace attrice in carne e ossa, ma all'ormai piuttosto diffuso worm che promette l'accesso esclusivo a foto senza veli della suddetta e di altre dive del momento, come Shakira e Britney Spears. Facendo clic sui finti link, oltre a non vedere nessuna foto piccante, già di per sé motivo di disappunto, si attiva il virus W32/Igloo-15, che installa una backdoor sul sistema, aprendo quindi una via di ingresso a semplici curiosi o malintenzionati vari.

GPRS E MMS NON TIRANO

I cosiddetti 2.5G, ovvero i cellulari GPRS e MMS, non hanno avuto il successo di pubblico sperato, nonostante l'impressione possa essere contraria: se ne parla molto ma se ne comprano davvero pochi. E questi non sono certo i presupposti migliori all'imminente (seppur imminente da molto tempo, e ora si comprende perché) lancio in larga scala di UMTS. Secondo le agenzie di marketing, la gente ha l'impressione che questi telefonini non servano poi davvero a molto, almeno per ora. Di certo c'è che il costo di GPRS è ancora alto per invogliare le masse.

PDA GPRS CON LINUX

Dall'azienda Invair è in arrivo, dopo l'anteprima al CeBIT 2003, un palmare ultrasottile, dalle dimensioni di una carta di credito. Linux Filewalker Messenger dispone di un sistema operativo basato su Linux e scheda GSM/GPRS triband, con viva voce e vibrazione. E' dotato inoltre di schermo a toni di grigi ad alta risoluzione, porta infrarossi, modulo GPS, interfaccia USB/RS232 e Bluetooth e uno slot Multimedia Card/Secure Digital. Il tutto a un prezzo di circa 649 euro (IVA inclusa).

PEER TO PEER NATIVO IN WINDOWS XP

E' stato appena rilasciato a cura di Microsoft un SDK (Kit di sviluppo software) dedicato agli sviluppatori di applicazioni peer to peer, che vogliano rivolgere i loro sforzi verso la piattaforma di Windows Xp. Tali applicazioni si baseranno su una nuova tecnologia, che sarà implementata come aggiornamento nel sistema, denominata Windows XP Peer-to-Peer Update, e che supporterà le applicazioni P2P sia centralizzate che decentralizzate, mediante l'aggiornamento delle API di Windows Xp per il supporto del protocollo Ipv6 e una versione migliorata e più flessibile del NAT.
Un interesse, già peraltro anticipato dal recente rilascio della versione beta di Threedegrees, un addon di supporto P2P per gli utenti di Windows XP e MSN Messenger, che potrebbe sembrare curioso, proprio da parte dei capifila della lotta allo scambio non autorizzato, dei paladini del diritto d'autore: ma il colosso di Redmond non perde d'occhio l'immensa utilità del sistema in un ambito aziendale, campo in cui già da qualche tempo Ibm e Sun si stanno muovendo.

XBOX LIVE PROMETTE BENE

La fase di betatesting europeo (effettuato in Francia, Germania e Gran Bretagna) del sistema di broadband online gaming per Xbox, ovvero Xbox Live Test Drive, cominciata il 28 novembre, sta per concludersi: per il 14 marzo è previsto il lancio ufficiale del sistema in Belgio, Francia, Germania, Italia, Olanda, Gran Bretagna, Spagna e Svezia. Nel corso dell'anno, le altre nazioni europee si aggiungeranno via via.
E pare che il sistema non solo funzioni, ma che sia anche molto soddisfacente, perlomeno a sentire le opinioni dei betatester: molto apprezzato, fra le funzionalità offerte dal sistema Xbox Live, il Voice Communicator, che dà ai giocatori la possibilità di interagire a voce con compagni di squadra e avversari durante le partite. Altre funzione molto apprezzate sono Optimatch, che consente di trovare, nella rete dei giocatori online, quello più adatto al proprio livello, non troppo abile né troppo pasticcione e Gamertag, una specie di identificatore universale e permanente che fornisce ai giocatori una ben precisa identità online, arricchibile e personalizzabile da parte dell'utente.

SUN CEDE AL FASCINO DI AMD

Neanche più i colossi del mondo RISC possono fare a meno dell'architettura pratica — e soprattutto a buon mercato — basata su x86. Questa è l'impressione che si ha, dopo la notizia dell'implementazione, da parte di Sun, dei chip a basso consumo AMD per i propri server di fascia bassa. Infatti, per i prossimi mesi sono previste in uscita due differenti linee di server blade: una tradizionalmente equipaggiata con UltraSPARC IIi da 650 MHz, e una dotata invece di Athlon XP-M (processori dedicati al mobile computing). Le caratteristiche dei processori AMD citati sono sembrate, evidentemente, imprescindibili per sistemi come i server blade, caratterizzati dal basso consumo e dall'estrema compattezza.
La piattaforma Solaris/SPARC resta comunque, Sun ci tiene a precisarlo, lo standard per i sistemi a 64 bit, in vista soprattutto delle novità dovute all'implementazione, su UltraSPARC, della tecnologia Throughput Computing. Ciò denota indifferenza, perlomeno momentanea, per Opteron, il processore a 64 bit in imminente uscita da parte di AMD.

OPERA PROIBITO AI POCKET PC

La saga delle ripicche fra Opera e Microsoft non sembra avere mai fine: quando ancora non sono spenti gli echi dello "scherzo" operato con la Bork Edition di Opera, che al posto del contenuto della pagina di Msn visualizzava parole dell'incomprensibile linguaggio del cuoco svedese del Muppet Show, ecco che Opera Software dichiara che mai il proprio browser potrà comparire sui telefoni o sui palmari basati sul sistema operativo Pocket PC. Non perché non credano nella possibilità di fornire un browser a uno smartphone, o nella bontà del loro browser (che fra l'altro implementa una tecnologia di renderizzazione video molto efficiente soprattutto per i dispositivi con schermi di piccole dimensioni), tutt'altro: proprio per quel motivo non vogliono contribuire, parole loro, al successo di Microsoft nel settore.

Opera Software si sta lanciando invece verso Symbian, che sta riscuotendo non meno successo di Pocket PC proprio nel campo degli smartphone. E' già pronta infatti una versione embedded di Opera per uno smartphone di Sony Ericsson, il P800. E pare ci sarà la possibilità di installare una versione gratuita di Opera anche sull'imminente 3650 di Nokia.

PERCHÉ PIACE LA MUSICA CHE PIACE?

Una domanda da cento milioni di dollari, direbbe qualcuno. E invece no: pare che un computer opportunamente programmato sia in grado di identificare al volo quali siano le potenzialità di successo di una canzone prima della sua uscita sul mercato. L'idea è di una software house spagnola, Polyphonic HMI, che evidentemente non crede nel principio secondo cui computer e frutti dell'umano ingegno non sono interfacciabili concretamente (vedi valutazione di opere d'arte o semplici traduzioni). Il programma in questione individuerebbe e analizzerebbe strutture e pattern matematici, alla ricerca di quelli che solitamente incontrano i gusti del pubblico, utilizzando una tecnologia pomposamente definita Hit Song Science (HSS).
La notizia strappa un sorriso all'utente medio, indubbiamente, ma non è così per le case discografiche più note, che anzi paiono essere già in trattative per verificare le effettive potenzialità del programma, il cui utilizzo si vorrebbe esteso, secondo le ambizioni degli autori, agli autori stessi. Ma tutti confidiamo che in pochi accettino di mettersi a produrre musica sinteticamente e matematicamente gradevole…

OFFICE SULLA RETE CON LINUX

Una annosa rivalità pare stemperarsi alla luce delle nuove esigenze di applicazioni client-server. In alternativa ai terminal server, due aziende, Codeweavers e Tarantella, stanno studiando in partnership soluzioni per accedere via HTTP alle applicazioni di Office automation di Microsoft. Saranno sufficienti un thin client Linux e un browser con supporto Java, nulla di più, e le applicazioni desiderate potranno essere utilizzate attraverso una interfaccia Web. Nella fattispecie, i protagonisti dell'operazione saranno due applicazioni già sviluppate dalle due aziende, Enterprise 3 di Tarantella, che fornisce l'accesso Web based e CrossOver Office di Codeweavers, che sfrutta la tecnologia di Wine per far funzionare sotto Linux le tradizionali applicazioni "da ufficio", come Lotus Notes e Office. Il loro connubio darà vita a CrossOver Office Server Edition, che permetterà di hostare applicazioni Windows su server Linux e accedere ad esse mediante un client Linux, senza bisogno di licenze supplementari.

HOT!

CELLULARE O WALKIE-TALKIE?

ERICSSON

SIEMENS

Ericsson, Nokia e Siemens hanno formato un consorzio per studiare e implementare nei loro dispositivi cellulari la tecnologia Push to Talk, che permetterebbe di utilizzare un telefono GPRS proprio come una radio ricetrasmittente, premendo un tasto per entrare in contatto diretto con l'interlocutore. Il consorzio dovrebbe unire gli sforzi e stabilire uno standard fin dall'inizio, per favorire l'interoperabilità, coinvolgendo via via quanti più soggetti possibile.

VENT'ANNI A UN CRACKER

La storia non è recentissima: nel 2000, un cracker kazako riuscì a violare i sistemi della celebre agenzia finanziaria Bloomberg (per intenderci, quella dell'attuale sindaco di New York) chiedendo poi 200.000 dollari per non rendere pubblico il cracking (che avrebbe potuto compromettere l'immagine dell'agenzia). Bloomberg, fingendo di accettare, ha allertato l'FBI, che si è presentato all'incontro per arrestare il cracker e il suo complice. I due, estradati negli Stati Uniti, rischiano ora guai grossi: per l'esecutore materiale si parla di una condanna che può arrivare a vent'anni di carcere!

UN AIUTO POCO COSTRUTTIVO

I bug di Windows diventano sempre più beffardi. L'ultimo si annida addirittura nella Guida in linea e supporto tecnico di Windows Me, attraverso la quale si può accedere a documentazioni, aiuto in linea e aggiornamenti vari. Gli URL utilizzati per tali puntamenti hanno prefisso hcp:// invece di http://, e proprio nel componente che gestisce questo genere di Url è annidato il buffer fallace che rende il sistema vulnerabile all'esecuzione di codice malizioso. Vulnerabilità purtroppo piuttosto frequente su vari componenti di Windows, ma per fortuna prontamente patchata dalla casa di Redmond.

NEWS

HOT!

GOOGLE: BLOGGER E NON SOLO

E' notizia di questi giorni l'acquisto di Blogger, il noto e utilizzatissimo portale per weblog, da parte di Google. Ma chi temeva che fosse l'inizio di un processo di espansione commerciale del motore di ricerca forse più utilizzato al momento attuale, deve ricredersi. Urs Holzle, il guru di Google, ha garantito all'impensierita stampa di settore che il portale che cura gode di ottima salute e di completa autonomia finanziaria, forte di oltre 500 dipendenti, grazie agli introiti pubblicitari e alla rivendita delle proprie tecnologie di ricerca. E che per questo intende restare un motore di ricerca e nulla più: niente portali multifunzionali, niente negozi, solo ricerca, più accurata e completa possibile, nell'ottica di una fruizione del Web semplice, utile e appagante. Ma, aggiunge anche, Google non diventerà mai un interprete del linguaggio umano: prima di tutto perché l'utente medio non vuole parlare con Google, porgli domande, ma semplicemente dargli in pasto parole chiave per vedere cosa riesce a trovare. E in tal senso Google cercherà costantemente di migliorare se stesso.

AUGURI DI BUON COMPLEANNO, BBS

Venticinque anni fa, a Chicago, ha cominciato la sua attività quella che è riconosciuta come la prima BBS (Bullettin Board System), ovvero niente più che un computer (uno Z-80) collegato a una linea telefonica mediante un modem a 300 baud. Su questo computer si raccolse piano piano una comunità, che prese a comunicare con le altre che si andavano formando mediante quello stesso modem, collegandosi al computer e ricevendo e inviando messaggi da una BBS all'altra. Le BBS sono gli antesignani pionieristici di tutte le forme di comunicazione telematica, e se ora ci strappano solo un sorriso nostalgico, allora erano un immancabile punto di ritrovo per molti.

SENDO PREPARA LA MARCIA SU MICROSOFT

Forse qualcuno si ricorda di Sendo e del suo amore finito con Microsoft: uno smartphone della succitata azienda, lo Z100, basato su Windows Powered Smartphone 2002, è stato bloccato da Sendo alla vigilia della commercializzazione per motivi mai del tutto chiari, e sfociati in battaglie di carta bollata in tribunale – si parla di furto di tecnologia e insider trading per portare al fallimento Sendo. Ora si passa al contrattacco: è in arrivo una linea di telefoni cellulari con display a colori, supporto EMS/MMS, suonerie polifoniche e giochi Java. Il primo a giungere sarà l'M550, più piccolo e economico dei modelli analoghi già sul mercato, e sarà presto seguito dall'attesissimo smartphone basato su Series 60 di Nokia. Un comunicato stampa sottolinea, forse con un fondo di sarcasmo, che le posizioni più liberali di Nokia in materia di codici sorgenti hanno fornito a Sendo grandi possibilità di personalizzazione dei dispositivi, nonché una maggior rapidità di sviluppo e un costo più basso del prodotto finito.

WIRELESS OLTRE GLI OSTACOLI

Parte da Singapore un ardito ma interessantissimo esperimento per la messa a punto della tecnologia wireless UltraWideBand (UWB), che è caratterizzata dall'emissione di singoli impulsi invece che di onde continue, con più impulsi corrispondenti a un singolo dato per avere la conferma di una corretta ricezione del segnale, arrivando a trasmettere fino a un milione di bit al secondo, con un consumo di energia ridotto rispetto alle tradizionali tipologie di trasmissione. I singoli impulsi, al contrario delle onde, non rimbalzano via contro muri e altre barriere che allo stato attuale della tecnologia si pongono come limiti invalicabili alla diffusione del segnale. La tecnologia, va da sé, è subito sembrata la soluzione ideale per applicazioni anche più peculiari, come il radar o il GPS. Ovviamente, con le dovute precauzioni per il rispetto della privacy del comune cittadino. Ma pare che, senza bisogno di pensare troppo in grande, questo genere di tecnologia sarà un toccasana per tutte quelle soluzioni, ambiziose ma mai davvero messe in atto, di reti wireless casalinghe così come aziendali.

PS2 SULLA GRIGLIA DI IBM

La tecnologia di grid computing di IBM, quella stessa che ha dato vita a innumerevoli e potenti computer virtuali in tutto il mondo, sarà utilizzata per il gaming online di Playstation 2, attraverso la piattaforma Butterfly Grid. Un network di questo genere, oltre a essere estremamente solido e sicuro, può sopportare il carico di milioni di giocatori su centinaia di piattaforme di gioco, e relativi picchi. In questo la strategia di Sony si differenzia radicalmente da quella di Microsoft, che ha creato un proprio network.

NOKIA A RISCHIO BLOCCO

Un SMS e un allegato vCard (lo standard per lo scambio di dettagliate informazioni sui contatti della rubrica, il classico "biglietto da visita") creato ad arte: questo basta per mandare in crash il Nokia 6210, causando anche altri fastidiosi effetti collaterali quali caratteri non validi sullo schermo o blocco totale di tutti i biglietti vCard. Sia chiaro, per tranquillizzare gli utenti, che anche il blocco più grave può comunque essere risolto semplicemente disconnettendo la batteria: nella maggior parte dei casi, semplicemente il telefono si riavvierà o sarà necessario spegnerlo e riaccenderlo.

I FONDI PER L'ECOMMERCE DURAN POCO

e-Commerce Incentivi per il commercio elettronico e per il collegamento telematico

Il 27 si sono aperte le iscrizioni per ottenere finanziamenti statali da investire nel commercio elettronico e nel collegamento telematico, per una somma totale di oltre 100 milioni di euro. L'iniziativa del Ministero delle Attività Produttive, era rivolta a tutte le imprese (si escludono le associazioni senza fini di lucro) che si occupano di hardware e software, consulenza, tutoring, formazione ed e-learning, per progetti di importo non inferiore a 7500 euro. Diciamo "era rivolta" perché, in realtà, nel giro di 24 ore l'accettazione delle domande è stata chiusa, per via dell'elevato numero di richieste, che ha esaurito nel giro di poche ore le risorse disponibili. Inutile dire che tutti coloro che non sono riusciti nemmeno a presentare la domanda in tempo utile sono parecchio arrabbiati e indignati della faccenda. Il problema principale è il meccanismo di accettazione delle domande, che blocca i fondi richiesti fin dalla presentazione della domanda; prevedibilmente, alcune domande non saranno accolte dal Ministero, e nessuno potrà quindi accedere ai fondi prima "prenotati" e poi negati. Insomma, oltre al danno del mancato finanziamento, ci sarà la beffa dei soldi che ci sono, ma non si possono ricevere. Per informazioni: www.legge388.info.

TELECAMERE A SCUOLA

Il fenomeno sta cominciando a Manchester, in Gran Bretagna, ma sta suscitando un interesse, è il caso di dirlo, piuttosto morboso, anche fuori dall'isola. L'idea nasce, si dice, dalla scarsa fiducia che i genitori ripongono nei rapporti dei professori sui loro figli, che a loro parere li dipingono molto più indisciplinati di quanto essi pensano che siano. Quindi, tranquillizza l'assessore che ha avuto l'ideona, non è nulla di persecutorio, solo un modo per dare una mano agli insegnanti e per arginare quell' 1% di studenti che, pare, rendono davvero difficile la vita ai poveri professori. Anzi, sarebbe un modo per stabilire un rapporto educativo più diretto fra insegnanti e genitori.
Il sindacato ha alzato più di un sopracciglio per questa iniziativa, ribattendo che una telecamera in aula farebbe sentire docenti e allievi un po' spiati, suscitando orwelliane memorie, e che più che di aiuto sarebbe di notevole impaccio. Ma l'assessore pare non sentire ragioni e ribattere sulla bontà didattica della sua iniziativa. Incrociamo le dita, sperando che queste alzate di ingegno siano limitate, e che il Grande Fratello, comunque lo si voglia intendere, resti fuori dalle aule scolastiche.

FA ANCHE IL CAFFÈ? NO. PER ORA.

Il nuovo pargolo di casa Nokia, il 3650, si presenta come un prodotto davvero allettante per gli appassionati di smartphone multimediali. Non mancano ovviamente il display a colori, la fotocamera VGA integrata con possibilità di trasmissione di immagini e video, il player RealOne per scaricare dalla rete e visualizzare video, il supporto MMS per inviare e ricevere messaggi completi di immagini, video e suoni e la tastiera dal design avveniristico, come ormai ci sta abituando la casa finlandese.
Anche la parte Pda è decisamente ben curata, con tanto di possibilità di sincronizzazione con Outlook e Lotus Notes.
Per quanto riguarda le applicazioni per Internet, è presente l'opzione di invio e ricezione di messaggi di posta elettronica, nonché un browser XHTML, attraverso il quale si può, oltre che navigare, consultare la guida turistica interattiva Lonely Planet, inclusa nel cellulare.
Il gioiellino è basato sul sistema operativo Symbian e supporta espansioni di memoria mediante memory card, ha cover intercambiabili e una vasta gamma di accessori, fra cui il supporto alla connessione mobile via Bluetooth.

HOT!

IL GARANTE FRENA GLI SPAMMER

Una delle scuse più frequenti utilizzate dagli spammer per giustificare la razzia di indirizzi di email e il loro conseguente, illecito utilizzo è "l'ho trovato in Rete". Ma il Garante per la Privacy ha sancito che il Web non è l'elenco telefonico, e che se un indirizzo di posta elettronica è presente online per un determinato motivo, ciò non significa che possa essere indiscriminatamente utilizzato per altri scopi. Lo spamming è illecito, a tutti gli effetti, e quindi sanzionabile: nulla di nuovo, ma evidentemente, se il Garante ha sentito il bisogno di stigmatizzarlo una volta di più, vuol dire che qualcuno ostinatamente non vuole capire.

EDITORI ONLINE IN CRISI

L'informazione a pagamento non paga, in Rete. Questo gioco di parole sottolinea adeguatamente i fatti che hanno portato alla fine dell'avventura, durata due anni, di Punto.com, uno dei giornali online più noti, anche per le sue peculiari modalità di pubblicazione, in versione cartacea e telematica al tempo stesso. E la stessa sorte sembra attendere Salon.com, forse la prima, sicuramente una delle più celebri ezine delle rete, che, seppur forte di quasi 50.000 sottoscrittori paganti, si trova in gravi dissesti finanziari.

IN IRLANDA DECOLLA LA FLAT. E QUI?

In Italia vige uno strano tabù sulle tariffe flat. Dopo la saga di Galactica (che non ha nulla a che fare con la fantascienza, purtroppo) e la conseguenza ridda di discussioni e prese di posizione in materia, a tutt'oggi non esiste, in Italia, un'offerta di connettività in modalità flat economica e dedicata a un pubblico di massa. In Irlanda, invece, si è mosso direttamente il garante delle telecomunicazioni, che ha pubblicato l'offerta, riservata agli operatori, per fornire connettività flat alla loro utenza. Si parla di un costo di 13 euro per utente, che potrebbe risolversi in un canone mensile di circa 30 euro.

CHI SONO E COSA PENSANO I TEORICI DEI VIRUS ARTISTICI

Artisti del virus

Sullo scorso numero abbiamo visto come in certi casi i virus possono essere visti come vere e proprie opere d'arte (e infatti ci sono musei che li espongono). E' venuto il momento di far parlare gli artisti!

Gli EpidemiC sono **i maggiori sostenitori della tesi secondo cui i virus non nascono necessariamente per scopi malefici** e non sempre sono dannosi o è loro intenzione esserlo. Per questi outsiders usciti da un romanzo cyberpunk di Neal Stephenson (così li ha definiti Arturo di Corinto) **"i virus non hanno altro comportamento se non quello che porta alla sua replicazione... La malvagità del virus deriva da una attribuzione d'intenzionalità socialmente condivisa. Il virus non ha alcuna intenzionalità"** (Michele Carparo). I virus si comportano con lo stesso modus operandi dei virus biologici: "si attaccano a un "organismo" per rimanerci e installarvi il proprio habitat, talvolta, e in casi più rari, per distruggerlo" (Giampaolo Capitani). **Il loro unico scopo dunque è esistere e moltiplicarsi** ma, come spiega lo zoologo Richard Dawkins, devono sottostare a due caratteristiche condizioni ambientali per riuscirci: "La prima è l'abilità del sistema ospite di copiare informazioni accuratamente e, in caso di errori, di copiare un errore con la stessa, identica, accuratezza. La seconda è la prontezza incondizionata del sistema ad eseguire tutte le istruzione codificate nell'informazione copiata".

Le origini del virus

Del resto se guardiamo più attentamente ai nostri giorni e un po' indietro nel tempo e consideriamo le aspirazioni dei primi programmatori di virus come di quelli odierni ci renderemo conto che **il virus non nasce con intenzioni maligne** tanto più che l'origine latina del termine rimanda sia a VIS (forza, vigore, energia, efficacia) sia a Viresco (verdeggiare, fiorire, essere vigoroso). Prima del 1986 gli esperimenti relativi ai virus **si verificano in ambiti strettamente accademici** e, a parte la curiosità per l'effetto visivo provocato da alcuni (si pensi al virus Ping Pong, creato al Politecnico di Torino, nel 1985), **sono finalizzati ad approfondire il concetto di programma auto-replicante e ad esplorare le analogie tra uomo e macchina**. Nel 1948 il matematico John von Neumann, crea un programma capace di agire proprio come i batteri di un'infezione all'interno degli organismi. In pratica può riprodursi autonomamente all'interno di un sistema, contaminandolo. Lo stesso concetto di programma auto-replicante riappare **dieci anni più tardi nel gioco Core Wars, sviluppato dai programmatori dei Bell Laboratories**. Lo scopo dei virus nel gioco è quello di riprodursi e distruggere altri virus. Il vincitore è colui che vanta il maggiore numero di virus riprodotti. Un programma che si auto-riproduce è qualcosa di molto simile ad una macchina intelligente, rende meno distante la prospettiva di **una vita e**

0100101110101101.ORG

www.0100101110101101.org
Se si raggruppa la sequenza di numeri, partendo da sinistra, in serie composte da 4 cifre, è possibile codificare grazie al codice esadecimale lo strano nome di questo collettivo. Il risultato è: 0100 = 4, 1011 = B, 1010 = A, 1101 = D

L' EPIDEMIA MEMETICA

Se siete interessati alla scienza del meme, particella elementare del contagio delle idee, se sognate una comunità della comunicazione, un "memeplesso" in continua evoluzione, uno spazio memetico e virale a tutti gli effetti, se aspira
te a diffondere e trasmettere i vostri memi in un'infezione digitale senza precedenti forse è il caso di dare uno sguardo a queste pagine.

Memetika
http://memetica.interfree.it
I Virus della Mente
www.virusdellamente.com

un'intelligenza artificiale, sogno umano che da sempre popola le pagine della nostra letteratura e anche gli schermi delle nostre sale cinematografiche.

>> Pro e contro

Verso questa visione però c'è anche chi ha manifestato dubbi e timori, **prospettando futuri alla Matrix** (dove Matrix, ricordiamo, significava, nel film ben noto a tutti, "controllo"). "Alle macchine potrebbe essere permesso di prendere tutte le proprie decisioni senza la supervisione umana - scrive Bill Joy - **sarà impossibile indovinare come tali macchine potranno comportarsi** (www.tmcrew.org/eco/nanotecnologia/billjoy.htm). I 0100101110101101.ORG, che invece in un'intervista dichiarano di essere interessati ancora a questo rapporto tra l'uomo e la macchina, affermano: **"L'arte della rete è prodotta da computer, non da uomini, siamo solo tecnici al servizio della macchina, addetti alla manutenzione.** La funzionalità di un computer è una qualità estetica: la bellezza delle configurazioni, l'essenzialità dei processi, l'efficacia del software, la sicurezza del sistema, la distribuzione dei dati, sono tutte caratteristiche di una nuova bellezza". Il loro obiettivo è divenire una cosa sola con il computer, fondersi con la macchina e diffondersi nella rete.
Il virus nasce anche come sfida intellettuale… sondare l'oscura topologia di Internet, tracciarne una mappa, esplorare la permeabilità della rete. "Un rizoma di tali e tante dimensioni come internet", afferma Jaromil, "non può essere rappresentato in nessuna topografia, ad oggi i tentativi sono stati molteplici, ma mai completi. La sua estensione può essere tracciata seguendo un cammino: **sondare i meandri, seguirne i percorsi e le connessioni**. Iniettare un liquido di contrasto nell'organismo per seguirne la conformazione e la struttura; al risalto otteniamo il percorso tipico dei vasi nell'angiogramma". **È grazie al virus che abbiamo scoperto l'esistenza della rete e il suo essere** "sommatoria di una serie di rapporti one to one"; il virus è "la prova ontologica dell'esistenza delle rete; niente poco di meno che la centralità della scrittura in una società che ama definirsi dell'immagine" (Gaetano La Rosa).

>> Information wants to be free

Il virus non è solo virus, ma anche **forma ultra moderna di comunicazione**, per nulla distinta dall'informazione stessa e il suo veicolo; **una forma di linguaggio**, un veicolo di trasmissione e dunque di comunicazione e persino informazione in sé e si sa che questo questo tasto è sempre stato a cuore agli hacker da divenire uno dei punti centrali della loro etica. Che il virus abbia l'abilità di diffondere informazione è stata ampiamente dimostrato da Sircam che, **dopo aver scelto un documento dall'hard disk, inviava tutti i dati, compresi quelli privati in esso contenuti agli indirizzi presenti nella rubrica del programma di posta elettronica**
Quando un virus riesce a invadere un sistema rivela in realtà anche un altro tipo d'informazione, e cioè **gli errori di quel sistema e come esso sia protetto in maniera sbagliata**. Insomma Ciò che occorre rimarcare – scriveva, nel post-I Love You, Andrea Vallinotto - è che non è di per sé il virus che "buca" le protezioni del sistema: di protezioni proprio non ce ne sono! (www.diff.org/diff/quattro/Loveyou.shtml)
Il virus, inteso come organismo autoreplicante, "è la cifra prima del linguaggio della rete che si esprime attraverso la contaminazione e l'ibridazione e che, trovato il vettore giusto, arriva a occupare ogni angolo di quel particolare spazio-tempo che è Internet, trasformandone forma e percezione" (www.epidemic.ws/d-i-n-a_press/il_manifesto.htm). Questo è il concetto base della teoria memetica di Dawkins, autore per altro del libro culto "The Selfish Gene" (1976), il quale, spiegando la storia della cultura sulla base delle teoria evoluzionistica di Darwin, dimostra come **il principio di "selezione naturale"** secondo cui sopravvivono solo quegli individui che

JAROMIL

http://dyne.org
Le ricerche di Jaromil, artista e programmatore italiano, residente in Austria, spaziano dall'ASCII ART allo Streaming Audio. Ha sviluppato il software Muse, un motore per l'encoding e il mixing di diversi streaming audio e lavorato allo sviluppo di un software video per Vjing rilasciato sotto licenza GPL.

CHI SONO E COSA PENSANO I TEORICI DEI VIRUS ARTISTICI

EPIDEMIC

www.epidemic.ws
Collettivo milanese di programmatori/artisti e artisti/programmatori. Per il resto amano non definirsi: [epidemiC] is not/ computer/web/net art / a computer scene product / an art scene product / a political attitude / a theoretical exercise / high tech / multimedial / interactive /[epidemiC] is not/ new / original / trendy

si riproducono con maggior successo di altri (vedi appunto il gioco Core war) **può essere esteso e applicato anche agli organismi culturali.** Come i geni sono delle unità contenenti informazioni biologiche e permettono la trasmissione dell'eredità biologica, così i memi sono entità contenenti informazioni culturali e permettono la trasmissione dell'eredità culturale. Se la diversità genetica è fonte di ricchezza biologica, allora anche **la diversità memetica è fonte di ricchezza culturale che risiede in pensieri differenti** e si scambia e si alimenta dalle comunicazioni interpersonali. I memi passano da un individuo all'altro e muoiono solo se si spezza la catena di trasmissione. I virus a loro modo funzionano proprio così; hanno la capacità di autoreplicarsi contaminando, e dunque trasmettendo, l'informazione in essi contenuta a un'altra entità. Tale caratteristica T. Tozzi la definisce "distribuiva" ed è anche tipica della comunicazione sociale con un'unica differenza, che "se si accetta di considerare fondamentale l'esistenza di un grado di interattività nella comunicazione, ci si accorge che nei modelli di comunicazione socio-culturale dominanti tale aspetto è spesso negato o trascurato" (strano.net/wd/mm_mz/museo001.htm).

>> Sabot & Sabotatori

Oggi la rete, considerata da sempre un gigantesco spazio di libertà, **rischia di essere piegata dalla logica del commercio** (e-commerce) e dell'economia (net-economy). Gli stessi programmi di igienizzazione e disciplinarizzazione, come li definisce Gianpaolo Capitani di epidemiC, portati avanti in nome della sicurezza dei pagamenti effettuati con la credit card, presentati come legittimi in quanto volti a servire meglio il consumatore e a preservare la privacy delle nostre comunicazioni, in realtà stanno gradualmente emarginando molte forme di attività, anche creative, della rete, **ostacolando la velocità con cui circolano le informazioni** (si pensi alla censura o al copyright), **limitando la diffusione di "pensieri differenti", la libertà di espressione e comunicazione di chi non vuol essere considerato un mero consumatore**. In questo contesto ecco che i virus appaiono come quei saboteurs, operai di origine belga, che bloccavano le macchine tessili lanciando un zoccolo (sabot) nel posto giusto; come **una forma di contropotere globale**, forma generalmente prepolitica che si oppone ai poteri forti, li riequilibria, li scompagina e li riassembla, come l'egemonia del comune e l'irruzione del sociale e in ciò che più sociale esiste; come il diritto allo **scambio non mediato dal denaro, la libertà del peer to peer,** il diritto all'open source, a napster, alla musica, alle notizie e in definitiva a un cosciente collettivo non riconducibile all'atto del consumo (Gianpaolo Capitani). Il virus insomma come ribelle atto poetico, così li definisce Jaromil, ma anche, sintomo politico e strutturale, tentativo di escursione della rete nella sua permeabilità; intelligenze artificiali che di rado sono dannose e che da

sempre popolano l'universo digitale, "poesie maledette", "giambi" rivolti contro chi vende la rete come un posto sicuro e borghese; composizioni spontanee, liriche nel causare l'imperfezione di macchine "fatte per funzionare" e nel rappresentare la ribellione dei nostri servi digitali.
Che altro dire? Forse – leggendo ancora gli epidemiC (Gaetano La Rosa), **i virus saranno davvero oggetti di consumo**, "distribuiti in varie forme e per varie utilità", forse l'utente un giorno avrà davvero un rapporto diverso con la macchina e non si farà più schiacciare "dalla brutale stupidità del poliziotto a una ridotta capacità espressiva del mezzo". E se è vero che "tutto, anche le immagini di un computer, ha alla sua base un testo scritto; e ultima, ma non meno importante, un'innovativa teoria teologica sulla genesi: **forse Dio per creare il mondo ha scritto un codice sorgente**".

DaMe`
www.dvara.net/HK

COSA SI NASCONDE NEL TUO PC?

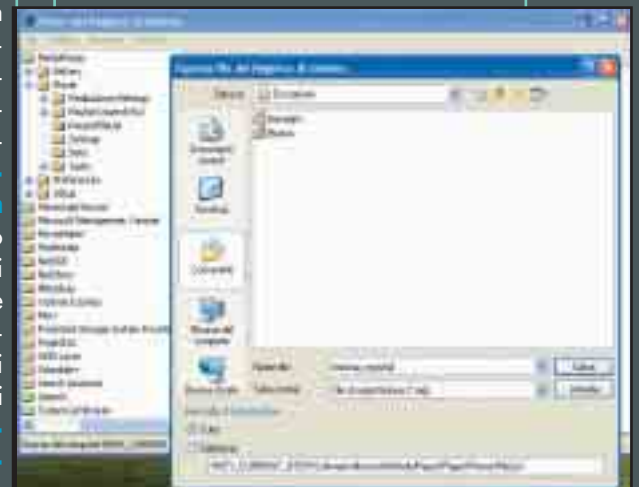
File aperti di recente, siti Web visitati, applicazioni utilizzate... Windows registra fin troppo meticolosamente tutte le operazioni che eseguiamo. Ecco come fare per riconquistare un po' di privacy.

Avete mai venduto un PC usato? O semplicemente un hard disk? Probabilmente vi sarete premurati di cancellare ogni dato sensibile: se siete stati accorti, oltre ai documenti e alle email, avrete ripulito anche la Cache dei file temporanei e la Cronologia da Internet Explorer, in modo che nessuno potesse vedere quali siti avete visitato. Potete quindi stare tranquilli che chi compra il vostro computer non potrà attingere a informazioni personali che vi riguardano? Mica tanto.

Spesso, cancellare la cache e la Cronologia di Explorer non basta a eliminare le informazioni personali dal computer.

>> Il registro di Windows

A volte, il nome di un file è sufficiente a rivelare ad altri informazioni che non vorremmo divulgare. L'esempio più ovvio è quello di immagini e filmati, diciamo così, sconvenienti. la presenza di un file che si chiama "contorsionista_tettona_bionda.avi" è abbastanza eloquente, per dirne una. Oppure, se sul computer del lavoro si trova traccia di un file "curriculum.doc", **il capo potrebbe capire che state cercando un nuovo lavoro**. Informazioni di questo tipo si possono facilmente trovare nei menu degli elementi recenti (quello che si trova nel menu File di molti programmi). Queste informazioni sono quasi sempre memorizzate nel Registro di Windows, ma **per cancellarle bisogna sapere dove andare a cercare**. Già, perché non tutte le applicazioni hanno un comando che permetta di ripulire queste informazioni.

Prima di vedere alcuni esempi, ecco una raccomandazione di rito: **il Registro di Windows è molto delicato**. Se si mettono le mani dove non si deve, e si modifica qualche elemento di troppo, **il computer potrebbe diventare inutilizzabile**. Per questo è importante fare una copia di backup del registro (da Regedit, selezionare Esporta dal menu File, accertarsi che l'Intervallo di esportazione sia impostato su Tutto, e salvare il file in una posizione sicura), e magari copiare i file più importanti.

Prima di lavorare col Registro, conviene sempre fare un backup completo, da ripristinare in caso di problemi.

>> Windows Media Player

Detto ciò, siamo pronti per aprire l'Editor del Registro di Windows. Dal menu Start, selezionate Esegui, scrivete regedit e premete invio. Si aprirà l'editor, nel quale possiamo andare alla ricerca delle chiavi incriminate, che sono memorizzate in ordine gerarchico, un po' come i file e le cartelle in Esplora Risorse. Partiamo con i **file recenti memorizzati da Media Player**. Le informazioni che ci interessano si trovano nella chiave HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player. I file aperti di recente sono memorizzati nella sotto-chiave RecentFileList; selezionate le voci File0, File1 eccetera, premete Canc e date conferma della cancellazione. Allo stesso modo, **si possono cancellare gli URL dei contenuti in streaming** riprodotti di recente (sotto-chiave RecentURLList).

Se dopo un po' vi siete stufati di continuare a eseguire queste operazioni, potete anche istruire Media Player a non memorizzare più i file aperti. Andate alla chiave HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Preferences. Se già non esiste, create un nuovo valore binario chiamato AddToMRU (clic col tasto destro nella parte destra della finestra, Nuovo/Valore binario, e inserite il nome). Fateci doppio clic, e inserite il valore 0 0 (quattro zeri saranno già presenti, per cui il risultato sarà quello mostrato nella figura "Far perdere la memoria a Media Player").

Le cattive abitudini di Windows Media Player **hanno effetto anche sugli utenti Mac**. Sebbene praticamente tutte le applicazioni create secondo le linee guida di Apple abbiano un comando per eliminare le voci del menu Elementi recenti, Media Player non ha questa funzionalità. Gli utenti di Mac OS X possono eliminare a mano il file ~/Library/Preferences/Windows Media Player Prefs, anche se questo avrà l'effetto di annullare tutte le preferenze di Windows Media Player.

Far perdere la memoria a Media Player. Modificando in questo modo il valore AddToMRU (o creandolo se non esiste), Media Player smetterà di registrare i file aperti nel menu degli elementi recenti.

>> Internet Explorer

Certe versioni di Windows 98 e Me, con Internet Explorer 5 non aggiornato, registrano la Cronologia e la cache in file nascosti e invisibili, che **rimangono sul vostro disco anche se scegliete di eliminare la cache e cancellare la Cronologia**. Quando diciamo "nascosto e invisibile", intendiamo dire che non si tratta di un "normale" file invisibile, che può essere tranquillamente osservato e aperto impostando le giuste opzioni in Windows (dal menu Visualizza di una finestra Windows, selezionare Opzioni cartella, poi Visualizza e nelle opzioni File nascosti selezionare Mostra tutti i file). Questi file sono infatti completamente invisibili dall'interno dell'ambiente Windows. **Solo se sapete dove andare a parare, potrete riuscire a vederli, copiarli in un altro punto del disco, aprirli da Windows, spaventarvi di ciò che vedrete, e finalmente cancellarli** definitivamente. Per più informa-

Se Explorer "fa il furbo"

Alcune versioni di Windows e di Explorer non cancellano effettivamente i file della cache e della cronologia quando si agisce sugli appositi comandi nelle Opzioni Internet. Per vedere se il vostro sistema è affetto da questo problema, seguite questi passi.

1 Aprite Explorer, andate su Strumenti/Opzioni Internet, e dalla linguetta Generale premete i pulsanti Elimina file… nel riquadro File temporanei Internet, e Cancella Cronologia dal riquadro Cronologia. Fate clic su Applica e poi su OK.

2 Dovreste aver cancellato ogni traccia residua delle vostre passate navigazioni, giusto? Mica tanto. Infatti, se andate su c\Windows\Temporary Internet Files, vedrete che ancora sono registrati tutti i cooky, che quasi sicuramente rivelano il sito che li ha emessi (potete arrivarci anche dalla finestra Opzioni Internet, facendo clic sul pulsante Impostazioni in File temporanei Internet e poi su Visualizza file… Poco male, direte voi: basta cancellare i file a mano. Ora dovreste essere tranquilli. Forse.

3 Se già il vostro computer non è impostato in questo modo, abilitate la visualizzazione di tutti i file, anche quelli nascosti e di sistema, come spiegato sopra. Ora osservate la vostra cartella dei file temporanei (c:\Windows\Temporary Internet Files, a meno che non la abbiate cambiata manualmente). Apparentemente, è vuota come il mio frigo al venerdì sera. Sospiro di sollievo? Niente affatto.

4 Se visualizzate la barra dell'indirizzo nella finestra di Windows, provate a inserire \Content.IE5 alla fine dell'indirizzo visualizzato. Notate qualcosa di strano? Windows non mostra alcun messaggio di errore. Invece, mostra il contenuto di una cartella che in teoria non esiste. Nella fattispecie, il contenuto è una finestra bianca, perché la cartella risulta vuota. Ma siamo davvero sicuri?

5 Provate ora a fare un'altra aggiunta al percorso mostrato nella finestra. Dopo \Content.IE5 inserite \index.dat. Questo file, aperto con un editor di testo, mostrerà un elenco degli Url visitati. Tenete presente che state visualizzando un file che secondo Windows non esiste…

BCWIPE

Spesso gli utenti non sanno che cancellando semplicemente un file dal proprio computer questo non viene annullato permanentemente dall'hard disk. Se avete bisogno di cancellare completamente alcuni dati che non è sicuro lasciare nel proprio computer, un programma come BCWipe può essere molto utile.
Le informazioni cancellate da una memoria di massa di tipo magnetico rimangono per diverso tempo prima di essere effettivamente rese illeggibili del tutto o in parte. BcWipe viene in soccorso degli utenti che necessitano la sicurezza assoluta della cancellazione di un file, in modo che nessun altro possa in alcun modo recuperare le informazioni eliminate. Il programma si integra intimamente con Windows e con la sua shell (Windows Explorer), garantendo la cancellazione dei dati con una procedura di livello militare e provvedendo anche alla pulizia dello spazio libero disponibile su una o più memorie di massa. Tra le funzioni accessorie del programma ricordiamo la possibilità di schedulare gli interventi e la possibilità di cancellare lo spazio rimasto inutilizzato a livello di cluster, nel caso assai frequente che un file non occupi tutto lo spazio del cluster. BCWipe è BCWipe comprende diversi livelli di cancellazione fino agli standard del governo degli Stati Uniti. Con BCWipe è anche possibile pulire lo spazio libero della vostra unità del disco rigido.
BCWipe è gratis e potete scaricarlo da www.jetico.com/download.htm

zioni, leggetevi il riquadro dedicato a IE in queste pagine. Le ultime versioni di Windows ed Explorer non hanno questo problema, e cancellano effettivamente i file dal disco. Qualcuno potrebbe però insospettirsi se la Cronologia viene continuamente cancellata l'intera cronologia. È però possibile fare in modo che gli indirizzi inseriti nella barra di Explorer non compaiano quando si comincia a digitare un nuovo URL, **senza cancellare l'intera cronologia**. La chiave di registro che ci interessa questa volta è HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs. Lì si possono vedere gli indirizzi digitati in IE, ed eliminare solo quelli incriminati. Attenzione però: questo ha effetto solo sugli indirizzi digitati (non sui link seguiti) e non rimuove questa informazione dalla Cronologia o dalla Cache di Explorer. L'informazione quindi **potrebbe essere comunque recuperata** da un utente malizioso e preparato sull'argomento.

>> File e applicazioni

Windows stesso tiene traccia di tutti i file e le applicazioni aperte da ogni utente. Gli effetti più immediati sono la visualizzazione di questi elementi nel menu Start/Documenti recenti, ma le informazioni potrebbero essere sfruttate in vario modo. Per escludere questa funzionalità per l'utente attualmente collegato, bisogna andare alla chiave di Registro HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer, creare un nuovo valore DWORD chiamato NoInstrumentation e dargli valore 1. Per applicare la stessa modifica all'intero sistema (e non solo all'utente attuale), applicare la stessa modifica a
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer. Affinché la modifica abbia effetto, bisogna riavviare il computer (o ricollegarsi con l'utente attuale, se la modifica è stata applicata solo a questo).
Ovviamente, questa modifica **potrebbe limitare le funzionalità di alcuni programmi** o elementi del sistema che devono accedere alla lista dei programmi o dei documenti usati di recente. Se trovate che la modifica altera in modo negativo il funzionamento di alcuni programmi, potete rimuovere il valore appena creato e riavviare il computer.

PURGEIE

Molti siti su Internet usano i famosi Cookie, i biscottini lasciati sul PC per memorizzare delle informazioni direttamente sul disco fisso del navigatore. Per leggere questi cookies dovete conoscere sotto quale nome sono stati registrati (se il computer di Nicola usa un carrello per acquisti per impostare un cookie che ricordi cosa dovete comprare, userà "NicolaCart=MB1450, Cyrix200" in modo da ricordare cosa avete nel vostro carrello. Per leggere il cookie devono leggere specificatamente il "Carrello Nicola". PurgeIE è un programma progettato per aiutare a mantenere i cookie e i file di cache per Internet Explorer. I file primari INDEX.DAT sono mantenuti senza richiedere un ricaricamento. C'é un'opzione per cancellare i cookie e i file di cache parassiti ed un'opzione per cancellare i file temporanei di Windows. PurgeIE serve anche come "Track Cleaner" per impedire ad altri di vedere la lista dei siti visitati di recente. L'opzione Preview permette di mostrare il risultato di ogni operazione Purge prima della sua esecuzione. PurgeIE può sostituirsi alla 'Pulitura disco' di Windows ed effettuare una migliore pulizia di cookies, URL visitati, file temporanei, dati recenti. PurgeIE è freeware e potete trovarlo sul numero di Aprile di Hackers Magazine, oppure scaricarlo da www.purgeie.com/download.htm
Se vi interessa studiare e imparare al meglio tutte le funzioni e le caratteristiche di PurgeIE è disponibile un tutorial molto dettagliato ma in inglese al sito:
http://aandrc.com/purgeie/tutorial/tutorial.htm

CONTROLLARE IL MAC DA UN CELLULARE BLUETOOTH

RADIOCOMANDO PER IL MAC

Sony Ericsson Clicker: la genialità fatta software

A volte tutti gli elementi sono già lì, sparsi sul tavolo. Serve solo qualcuno che li metta insieme, magari con **quel pizzico di genialità che fa sì che gli elementi si combinino in un modo che nessun altro aveva mai intuito prima**. Più o meno è quello che ha fatto Jonas Salling, che ha preso pezzi di

Sony Ericsson Clicker si installa come pannello delle Preferenze di Sistema. Il programma costa 12,95 dollari, e lo si può scaricare da http://homepage.mac.com/jonassalling/Shareware/Clicker.

tecnologie già presenti e ben note, e li ha ricombinati in modo originale.
Stiamo parlando dell'applicazione Sony Ericsson Clicker, un programmino che utilizza bluetooth, le funzionalità di gestione degli accessori esterni da parte dei cellulari Sony Ericsson, ed AppleScript, il sistema di automazione di Mac OS. Con tutti questi ingredienti, è possibile **trasformare il proprio telefonino in un telecomando che permette di eseguire qualsiasi sul proprio Mac operazione sia gestibile via AppleScript** (tra queste, lo ricordiamo, ci sono anche comandi e script di shell… moooolto interessante).
Bluetooth è un sistema di comunicazione senza fili, tipo quello a infrarossi, che permette di mettere in comunicazione apparecchi di tipo diverso e sfruttarne le funzionalità. Per esempio, con un computer e un cellulare dotati entrambi di trasmettitori bluetooth, si può collegare a Internet il computer usando il cellulare, scambiare indirizzi e numeri di telefono e molto altro.

>> I principi di funzionamento

Alcuni dei telefoni Sony Ericsson (T39, T68…) hanno probabilmente la migliore implementazione bluetooth sulla piazza. Tra le varie funzionalità previste, c'è quella di poter **pubblicare su un apparecchio un menu che comandi le funzioni dell'altro**. In pratica, l'apparecchio A dice all'apparecchio B qualcosa tipo "Se vuoi, io so fare queste cose: alzare il volume, abbassarlo, disabilitarlo". Sull'apparecchio B, apparirà quindi un menu con il nome dell'accessorio, e vari comandi per le funzioni "pubblicate". Il programmino fa proprio questo: definisce una lista di funzioni e comandi, e li invia al cellulare. **A ogni comando, può essere associato un qualsiasi AppleScript**, che comanda azioni semplici o molto complesse sul Macintosh. Di default, Clicker viene fornito con quattro set di comandi per iTunes, DVD Player, PowerPoint e Keynote (la nuova applicazione per presentazioni di Apple); fin da subito è possibile quindi **avviare o interrompere la riproduzione di un CD, un file Mp3 o un DVD**, passare alla traccia successiva, regolare il volume, e controllare la sequenza di diapositive di una presentazione.

>> Creatività senza limiti

Ciliegina sulla torta, Clicker ha anche **un "sensore di prossimità"** che permette di eseguire una qualsiasi azione nel momento in cui il cellulare entra o esce dal campo di azione dell'antenna Bluetooth (10 metri circa, in condizioni ottimali). Si può quindi fare in modo che **il computer vada in stop o attivi il salvaschermo con password se ci si assenta dalla stanza**, oppure che ci saluti educatamente quando entriamo (o scarichi la posta, o lanci la sincronizzazione dei dati col telefono o il palmare).
La chiave di volta, lo ripetiamo, è la versatilità: qualsiasi azione pilotabile via AppleScript può essere attivata da un menu sul cellulare.

Grazie al sensore di prossimità, il Mac esegue azioni quando ci avviciniamo o ci allontaniamo.

>> E quello che non si può scriptare?

Inevitabilmente, arriva un momento in cui l'entusiasmo per Clicker si smonta. **Il programma infatti sembra essere inutilizzabile proprio in una delle sue applicazioni principe**: l'utilizzo come vero e proprio telecomando per guardarsi in TV i film codificati in DivX. I migliori programmi per visualizzare i DivX (Video Lan Client e MPlayer OS X) sono infatti "portati" dal mondo Unix, e **non supportano AppleScript**. Non è il caso di disperarsi. Mettete da parte momentaneamente i pop-corn e attaccatevi a Internet, perché la soluzione c'è ed è a portata di mano. Apple ha recentemente rilasciato un'estensione per AppleScript chiamata **GUI Scripting, con cui si può pilotare qualsiasi elemento nell'interfaccia di quasi tutte le applicazioni per Mac OS**. Ecco l'uovo di Colombo. Andate quindi su www.apple.com/applescript/GUI e scaricatevi la beta del software necessario. Installatelo sul vostro Mac e attivate "Abilita accesso per dispositivi di assistenza" nel pannello "Accesso Universale" di Preferenze di Sistema. Siete pronti per pilotare MPlayer via AppleScript.

>> Telecomando e TV

Aprite il pannello SonyEricsson Clicker in Preferenze, e selezionate la linguetta **Phone Menu**. Dalla colonna **Available Items**, trascinate l'elemento **Menu** nella colonna di sinistra. Chiamatelo MPlayer (o come diavolo volete). Ora andate nella linguetta **Actions**, premete su **Add Action** e, nella parte di destra, inserite il seguente codice:

```
– Play/Pausa
tell application "System Events"
  tell process "MPlayer OS X"
    tell window "MPlayer OS X"
      click button "Play"
    end tell
  end tell
end tell
```

Date un nome all'azione appena creata (con un doppio clic sulla colonna di sinistra). Ora, allo stesso modo, create altre azioni sostituendo di volta in volta la riga con il comando **click button**, in questo modo:

Avanzamento rapido 10 secondi:
`click button "»"`
(il carattere "»" si ottiene con Alt+Shift+1 nelle tastiere Italiano Pro)
Riavvolgi 10 secondi:
`click button "«"`
(il carattere "«" si ottiene con Alt+1 nelle tastiere Italiano Pro)
Attiva/Disattiva sottotitoli:
`click button 8`
Visualizza a tutto schermo:
`click button 9`
Visualizza informazioni sul tempo della traccia:
`click button 11`

Fate attenzione a una cosa: a seconda delle versioni e della distribuzione, il nome del programma cambia (Mplayer OSX tutto attaccato in alcuni casi, OS X staccato in altri). Fate in modo che il vostro script chiami l'applicazione col suo vero nome.
Bene, se avete fatto tutte le azioni, siete pronti ad andare nella sezione **Phone Menu** e trascinarle nel menu MPlayer creato in precedenza. Premete su Publish e il nuovo menu comparirà nella voce **Accessori** del telefono. Adesso correte pure al divano a provare il tutto, con pop-corn, coca cola e cellulare.

>> Approfondiamo un po'

Ok, giochino del telecomando a parte, quello che abbiamo appena visto **è molto più importante di quello che sembra**. Con il GUI scripting si possono comandare via AppleScript anche applicazioni che normalmente non sono scriptabili, o che lo sono in modo limitato, purché abbiano un'interfaccia grafica nativa per Mac OS X. A parte alcune rare e lodevoli eccezioni, l'implementazione di AppleScript in Cocoa lascia un po' a desiderare. **Il GUI scripting risolve questi problemi**, e vale la pena di conoscerlo un po' meglio. Osserviamo la prima parte del listato:

```
tell application "System Events"
  tell process "MPlayer OS X"
    tell window "MPlayer OS X"
      click button "Play"
```

A differenza dei normali AppleScript, l'espressione tell **non si riferisce al programma da pilotare**, ma sempre e solo all'applicazione "System Events". Sarà questa poi a navigare i vari menu ed elementi di interfaccia del programma destinatario, fino ad arrivare all'elemento da selezionare. **Ma come si fa a conoscere i nomi delle finestre, dei menu e dei singoli controlli? A** volte sono espliciti (il titolo di una finestra, per esempio), ma altre volte sarebbe necessario analizzare il sorgente dell'applicazione per sapere come il programmatore ha chiamato il singolo pulsante. Fortunatamente, Apple ci viene incontro con il programma UIElementInspector, che si scarica da www.apple.com/applescript/GUI/UI-Inspector.sit. Questo programma **apre sullo schermo una finestra che mostra il nome dell'elemento di interfaccia su cui si trova il puntatore del mouse**, insieme ai nomi di tutti gli elementi padre di quell'oggetto e altre informazioni, come le coordinate del mouse. E ora, sotto con gli script!

UIElementInspector rivela le coordinate fisiche e logiche di ogni elemento dell'interfaccia di un'applicazione Cocoa.

FREENET: IL PEER 2 PEER ANONIMO, CIFRATO, INATTACCABILE

LA RETE DAVVERO

Concludiamo il nostro viaggio nel mondo del peer to peer con qualcosa di diverso e più ampio da ciò che abbiamo visto finora, nelle sue applicazioni e soprattutto nella sua filosofia.

Freenet è, in linea di principio, una applicazione peer to peer basata su Java, né più né meno di quelle che abbiamo visto finora. Eppure, al tempo stesso **è qualcosa di completamente diverso**. Si distacca infatti dalla usuale logica di caccia alla canzone o al film, per instaurare una vera e propria cultura della condivisione. Freenet si autodefinisce come un "enorme contenitore virtuale di informazioni", quando non addirittura "l'Internet alternativo", in cui si può essere **fornitori di contenuti o semplici nodi di passaggio delle informazioni, libero e aperto a tutti**. Le informazioni sono protette nella loro integrità e nella loro anonimità dalla stessa struttura del network, nonché da **robusti algoritmi di cifratura, e sono consultabili velocemente e liberamente senza timori di tracciature di alcun genere**. Nasce nel 1999, su un progetto di Ian Clarke per distribuire e reperire informazioni in un sistema decentralizzato, e da allora, dopo aver attirato gli immancabili strali dei protettori del diritto d'autore, è andato evolvendosi fino all'attuale versione.

Uno dei passi dell'installazione di Freenet, dal quale si possono scegliere i componenti da installare.

>> Installare Freenet

L'installazione è estremamente semplice e lineare. Da http://freenet.sourceforge.net, il sito del progetto (una versione italiana del sito è reperibile presso http://freenetproject.org/cgi-bin/twiki/view/IT/WebHome) si scarica l'installer per Windows o per altri sistemi, che reperirà poi i file necessari. In caso di difficoltà, si può scaricare l'installer completo della versione più recente dei file di installazione, detto "snapshot" (procedura da seguire comunque per l'installazione sotto Linux e Macintosh). Da lì si procede semplicemente approvando le varie fasi del setup. Verranno quindi installate le runtime Java necessarie, e nella barra degli strumenti sarà visibile la simpatica iconcina di un coniglietto azzurro stilizzato in corsa.

>> Configurare Freenet

L'ultima cosa necessaria a far partire il nodo Freenet è il Node Ref, abbreviazione di Node Reference, ovvero una chiave di riferimento nel network. **È una delle basi della riservatezza di Freenet**: nella maggior parte dei casi si può accettare quella di default, ma ci sono casi in cui un provider o un governo può aver individuato la chiave di default come appartenente a Freenet, e averla quindi bloccata. In questo caso, si dovrà ottenere la chiave da un altro noto, per **bypassare il blocco e sfuggire ai controlli**. Tutti coloro ai quali la frase "sfuggire ai controlli" abbia fatto storcere il naso, sono invitati a leggere il paragrafo sulla filosofia di Freenet…

Un clic destro sull'icona permette inoltre di importare ed esportare Refs, definire il nostro nodo come transiente o permanente, chiudere, fermare e riavviare Freenet, visualizzare il log (in cui sono registrate tutte le operazioni effettuate dal nodo) e accedere ad altre configurazioni particolari (riservate ai più che esperti).

>> Utilizzare Freenet

Un doppio clic sull'icona apre il nostro browser di default con l'interfaccia Web di Freenet. Sulla sinistra, ci sono una serie di strumenti informativi: **connessioni aperte, carico del network, task in opera, conclusi e falliti, ambiente operativo e opzioni** da linea di comando. Al centro, la sezione dei bookmark riporta i link ai principali indici di siti Freeweb, reperibili direttamente da lì o attraverso la finestra di ricerca immediatamente inferiore, in cui la ricerca deve essere effettuata attraverso la chiave Freenet corrispondente, qualcosa come **freenet:MSK**@**SSK**@[**chiave alfanumerica] /cartel-**

LIBERA

Freenet si manifesta a noi sotto forma di interfaccia Web, dentro al browser predefinito.

la//pagina.html.
Più sotto ancora, la possibilità di inserimento di risorse Freeweb, nel caso volessimo **inserire noi stessi qualcosa nella rete**, con relativo Time To Live e indicazione della tipologia Mime del file.
E proprio parlando di Mime, dobbiamo fare una precisazione: se utilizziamo Internet Explorer, a ogni richiesta comparirà (se non disabilitata come da istruzioni) una pagina di avviso, che ci avvertirà che **stiamo utilizzando uno strumento potenzialmente non sicuro**. Molto semplicemente, Internet Explorer non interpreta correttamente i modelli Mime, compromettendo la sicurezza e la stabilità dei passaggi di informazioni. Problema da cui è immune, per dirne uno, Mozilla.

>> Applicazioni per Freenet

In questo momento l'applicazione più interessante è sicuramente la pubblicazione su Freenet di siti Web aggiornabili in tempo reale (weblog, bollettini). Esistono a tal scopo guide esaurienti (la più nota è reperibile su Freenet all'indirizzo **freenet:MSK@SSK@enI8YFo3gj8UVh-Au0HpKMftf6QQAgE/homepage//website_HOWTO.html**), nonchè appositi script e utility, come FreeWeb (http://freeweb.sourceforge.net). Per gli utenti Linux, ne è disponibile una versione a linea di comando, FCPTools (**http://freeweb.sourceforge.net/fcptools.html**).
Inoltre è possibile leggere e inviare news attraverso la rete Freenet e il nostro usuale news reader mediante il programma FreeNews (**www.storrow.org/Software/FreeNews/**).

>> La filosofia di Freenet

La libertà è un principio discusso, a volte abusato, nella Rete come ovunque. E tutti gli strumenti che danno la libertà di andarsene in giro tranquilli e nascosti possono essere utilizzati come **un'arma a doppio taglio**: per cause nobili, interessanti, divertenti o niente di tutto questo. La rete Freenet è come una grande arteria stradale: ci viaggiano le famigliole in vacanza come i criminali. Ma **non per questo le strade dovranno mai essere sbarrate**. Ugualmente, Freenet è uno strumento, usabile e abusabile, da lodare per i suoi utilizzi nobili più che da vituperare per quelli meno nobili.
Freenet **fa circolare prima di tutto informazione**. E per Ian Clarke l'informazione è la base stessa della libertà, di ogni genere di libertà. L'informazione libera, accessibile a tutti e non manipolata da nessun governo o parte politica. Accessibile e veicolabile: perché tutti sappiano, tutti devono poter dire, e per poter dire, tutti devono essere liberi di esprimersi in modo anonimo, o meglio, attraverso pseudonimo (che, grazie alla firma digitale, può divenire più sicuro e inequivocabile di qualsiasi nome), senza temere ritorsioni.
E il copyright? Superabile, secondo i seguaci di Freenet, che anzi già lo danno per morto, vinto dalle nuove forme di comunicazione e scambio in Rete: la proposta è quella del cosiddetto Fairshare, ovvero una sorta di mecenatismo moderno, basato su offerte spontanee da parte degli utenti (collegati, nemmeno a dirlo, attraverso la rete Freenet) verso gli artisti di loro gradimento.
Su Freenet sono reperibili gli scritti di autori e giornalisti "silenziati", le inchieste che "scottano" e danno fastidio ai vari governi, ma anche le release di Linux "sicure". Su Freenet chiunque può pubblicare senza disporre di uno spazio Web, grazie alla disponibilità dei vari nodi della rete. E soprattutto, **nessuno, neanche Ian Clarke, può controllare o fermare quello che gira per la rete Freenet.**

Paola Tigrino

Manco a dirlo, uno dei browser che può compromettere la sicurezza e l'affidabilità delle comunicazioni di Freenet è –guarda caso– Internet Explorer. Un motivo in più per cambiarlo.

PANICO PRIMA DEL

Una serie delle più frequenti domande che assillano le persone che vogliono installare Linux sul proprio computer e non hanno mai visto niente di diverso da Windows.

Vorrei installare Linux ma tutto lo spazio su hard disk è occupato interamente dalla partizione di Windows 98; è possibile farlo senza dover ripartizionare da capo l'hd?

Esistono diversi programmi che permettono di ridimensionare facilmente una partizione Fat32, creando così spazio libero per nuove partizioni. Sebbene non più attivamente sviluppato e quindi caduto un po' in disuso, **Fips** (www.igd.fhg.de/~aschaefe/fips/) rimane uno dei programmi che hanno aiutato generazioni di utenti a ritagliare sempre più spazio per il pinguino sul proprio disco fisso. Ufficialmente supportato dal progetto GNU e in fase di sviluppo è invece **Parted** (www.gnu.org/software/parted), in grado di ridimensionare partizioni di tipo Ext2 e Fat. Inoltre le più note distribuzioni integrano appositi tool grafici utilizzabili in fase di installazione per semplificare ulteriormente il processo di ripartizionamento; tra questi spicca sicuramente **DiskDrake**, incluso con la distro francese Mandrake. Prima di avviare il processo di ripartizionamento, è consigliabile effettuare un Defrag per compattare i dati e ridurre al minimo la loro frammentazione nel disco rigido; inoltre effettuate un backup preventivo dei vostri preziosi dati poichè, come ogni bravo informatico sa… la legge di Murphy è sempre in agguato, e se qualcosa può andar male, lo farà senz'altro ;-) Infine, se sull'hard disk sono presenti partizioni NTFS di Windows NT/2000 o XP, è necessario ahimè ricorrere a software commerciali come **Powerquest Partition Magic** per ridimensionarle.

Problemi con Linux? Il forum sul nostro sito vi attende!

Volevo sapere se esiste un modo per accedere direttamente da Linux ai dati presenti sull'altra partizione di Windows, ad esempio nella cartella C:\Documenti\...

Abbiamo già avuto modo di parlare delle particolarità del filesystem di Linux sul numero 18 recentemente pubblicato. In questo caso sarà sufficiente montare la partizione di Windows nel filesystem; il punto di montaggio predefinito, a volte /windows e a volte invece /mnt/windows, può variare in base alla distribuzione. Ad esempio con il comando

```
$ mount /dev/hda1
/mnt/windows
```

sarà possibile accedere ai dati presenti in C: entrando nella directory /mnt/windows. Inoltre il comando mount cerca di riconoscere il tipo di filesystem che si sta montando, anche se con l'opzione -t <tipo-fs>, -t vfat nel nostro caso, è possibile specificarlo direttamente. Infine con l'opzione -r il dispositivo verrà montato in sola lettura. Ad esempio

```
$ mount -t iso9660 -r /dev/hdc /mnt/cdrom
```

Una volta acquisita un po' di dimestichezza con le partizioni e il loro montaggio, potrete personalizzare il file /etc/fstab in base alle vostre esigenze, semplificandovi notevolmente la vita. Sappiate infine che le partizioni di Windows NT4/2000/XP non sono di tipo Fat32 bensì NTFS: questo implica che il tipo di filesystem è ntfs e, soprattutto, **sono accessibili solo in lettura.**
Ultimo ma non meno importante, **assicuratevi sempre di aver smontato correttamente i dispositivi una volta finito di utilizzarli**, con il comando umount (non è un er-

GRANDE PASSO

L'unione fa la forza: i gruppi di utenti

La tendenza "sociale" dell'uomo, il suo bisogno cioè di incontrarsi e confrontarsi con altri individui in cui si riconosce e con i quali condivide qualcosa, trova ampi spazi anche in settore come l'informatica e, in particolare, con il software libero. Alle vivaci comunità virtuali di utenti e sviluppatori che si formano intorno ad ogni porzione di codice free, esistono sparsi per tutto il mondo migliaia di Linux User Group. Un LUG altro non è infatti che un gruppo di persone accomunate da una stessa passione e che collaborano insieme condividendo esperienze, ampliando le proprie conoscenze e che si impegnano attivamente per promuovere il software libero sul territorio locale. Per fare questo i LUG, oltre ad impegnarsi nella creazione di una comunità virtuale (ove gli utenti interessati possono richiedere informazioni o, perchè no, un aiuto..), organizzano spesso corsi, incontri con studenti, meeting, giornate "a porte aperte" quali il noto LinuxDay e persino mega grigliate! Per sapere quale è il Linux User Group più vicino a casa vostra, potete consultare la lista disponibile all'indirizzo www.linux.it/LUG/

rore, la n si è persa per strada...)

```
$ umount
<dispositivo>
oppure
umount
<punto-mon-
   taggio>
```

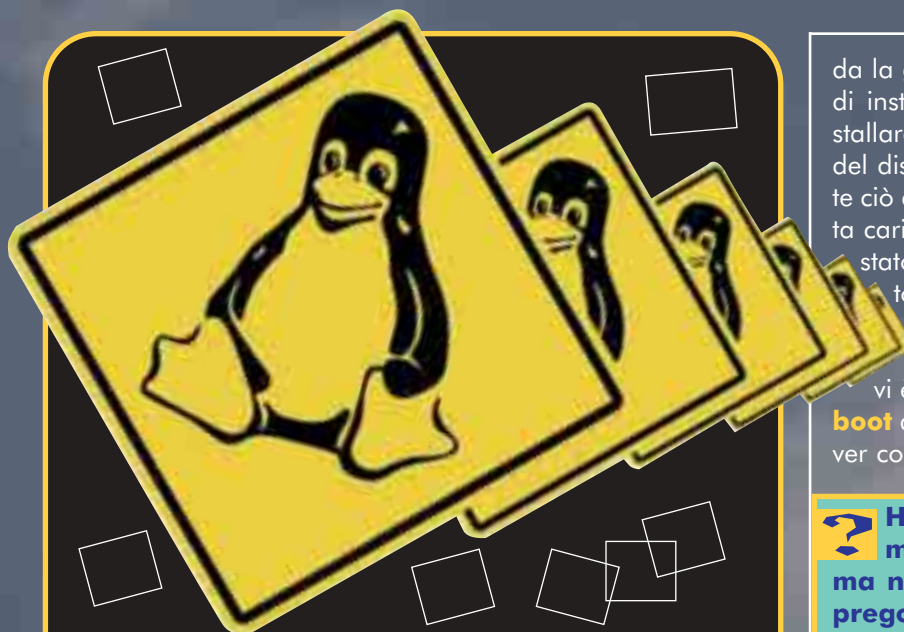
Come posso utilizzare sotto Linux i diversi programmi che normalmente utilizzo con Windows? C'è qualche emulatore?

WINE (www.winehq.com) è oggi forse il più noto pacchetto per l'interoperabilità Linux/Windows; compito di questo software non è infatti quello di emulare il noto ambiente Microsoft bensì quello di **fornire un implementazione open source delle API (Application Programming Interface) di Windows per sistemi Unix-like**. Più nel dettaglio, Wine (che sta per WINdows Emulator ma anche per WINE Is Not an Emulator!) fornisce un loader che, appoggiandosi ad apposite librerie, traduce le chiamate dei programmi per Windows in chiamate per Linux/X-Windows. Un approccio diverso è invece quello di **Bochs Emulator**, che non si limita ad supportare il sistema di Redmond bensì emula un intero PC, dal BIOS ai vari dispositivi.

Altri programmi utilizzabili per scopi simili sono **Win4Lin, VmWare** o **Codeweavers CrossOver Office**: in questo caso però non si tratta di software libero ma commerciale.

È importante però notare come l'emulazione non **sia nella maggior parte dei casi la soluzione migliore**: di molti programmi open source per Windows è stato effettuato un porting verso piattaforma Linux (anzi.. spesso accade il contrario!) e, in altri casi, sono stati sviluppati appositamente dei "cloni" per Linux che, quasi sempre, superano sotto molti aspetti il programma originale.

Purtroppo dispongo di un solo PC e non vorrei rinunciare completamente a Windows, pur volendo sinceramente provare Linux: come posso gestire questa "convivenza forzata"?

Quasi sempre Windows e GNU/Linux risiedono in partizioni differenti e quindi indipendenti, e quindi l'unico problema riguar-

Considerato che altri prodotti commerciali potevano vantare grosse quantità di documentazione, molti utenti decisero di unire i loro sforzi e lavorare insieme per fornire, mantenendo stretti contatti con i programmatori, una documentazione completa e di qualità sul sistema GNU/Linux fondando così il Linux Documentation Project.
La biblioteca del Ldp (www.tldp.org/) è divisa in varie categorie:

- **HOW-TO (letteralmente "come fare per...")**: tantissimi e focalizzati alla risoluzione delle problematiche più disparate legate alla configurazione di un particolare aspetto del sistema piuttosto che di una periferica hardware; per ogni vostro problema esisterà probabilmente un How-To in grado di aiutarvi a risolverlo!.

- **Guides:** le guide non sono nient'altro che libri nel vero senso della parola tanto che, alcune di quelle ivi presenti, sono anche state stampate in formato cartaceo da editori di fama come O'Really Associates o, in Italia, da Hops Libri e Apogeo; se volete ad esempio amministrare un sistema o giocare un po' con il kernel, in questa sezione troverete pane per i vostre denti

- **FAQ (Frequently Asked Questions, ovvero le domande più frequenti):** divise per argomenti, sono state pazientemente raccolte le domande più ricorrenti poste alla comunità; si rivelano in particolare utilissime per una risoluzione rapida dei problemi più semplici.

- **man pages:** poteva forse mancare una sezione aggiornata delle pagine di manuale (le note "Man pages") dei comandi GNU/Linux più diffusi?

Anche noi Italiani disponiamo di un Ldp tutto nostro (http://ildp.pluto.linux.it/) che, grazie all'impegno di molti, ha messo a disposizione nella nostra madre lingua la maggior parte dei documenti prima presentati. Sono inoltre da segnalare diversi pregevoli lavori "made in Italy" (la cui lettura è consigliata vivamente ai principianti!) tra i quali spiccano gli "Appunti di informatica libera" di Daniele Giacomini, un completissimo manuale di milleduecento pagine riguardante ogni aspetto di questo SO, "Linux Facile" di Daniele Medri e "Linux da Zero" di Marcello Missiroli.

da la gestione del boot dei singoli sistemi presenti. In fase di installazione tuttavia le distribuzioni consentono di installare nel MBR (Master Boot Record, cioè il primo settore del disco) un **BootLoader**, un programmino che consente ciò di selezionare quale sistema operativo di volta in volta caricare; storicamente il bootloader per Linux è sempre stato **LILO** (LInux LOader) anche se recentemente è stato un po' messo in disparte e ad esso le varie distribuzioni stanno preferendo **GRUB**, forse più complesso ma decisamente più versatile. In alternativa vi è comunque la **possibilità di creare un floppy di boot** da utilizzare per l'avvio del Linux installato, senza dover così intaccare il MBR.

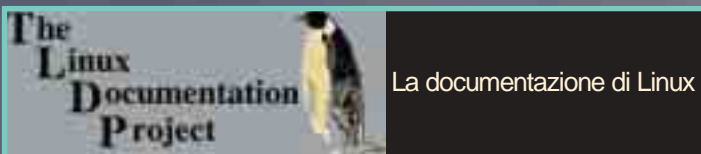
? Ho urgente bisogno di eliminare completamente Linux dal PC su cui lo avevo installato ma non ho assolutamente idea di come fare!!! Vi prego... aiutatemi!

Sebbene normalmente l'eliminazione di Linux comporti la fucilazione immediata, vedremo per questa volta di chiudere un occhio… ;-) Tra le diverse alternative possibili, la più semplice è forse quella di utilizzare il buon vecchio **fdisk di MS-Dos** per eliminare le partizioni Linux ed eventualmente **sovrascrivere il boot manager installato**. Chiunque fosse interessato può trovare sulla mia home page (www.muug.it/lele/) un documento intitolato "FDisk - Eliminare partizioni Linux" che spiega passo per passo cosa fare in questi casi.

? Come si utilizza il comando move? Volevo sapere quali sono le opzioni per ls? Quale è la sintassi del comando tar?...

Tradizionalmente la documentazione dei programmi sotto unix viene diffusa sotto forma di man(ual) pages, ovvero pagine di manuale in linea. **Il programma man consente di accedere alla documentazione disponibile** sul sistema in maniera estremamente semplice; digitando man seguito dal nome del programma su cui si desiderano maggiori informazioni, comparirà sullo schermo la pagina di istruzioni contenente tutti i dettagli. Per scorrere le pagine di manuale è sufficiente utilizzare i tasti cursore e le lettere u (up) e d (down), mentre per uscire utilizzate q; per avere ulteriori informazioni sul funzionamento di man e sulle pagine di manuale dovrete semplicemente scrivere... **man man!**

? Incuriosito dal progetto UnitedLinux, ho scaricato il CD e ho installato il sistema; purtroppo ho sbagliato qualcosa nella configurazione della grafica e ora ogni qualvolta avvio il sistema, tutto sembra caricarsi correttamente finché, alla fine, il monitor inizia ad accendersi e spegnersi più volte ed infine compare la scritta, in modalità testuale, "Login etc..". Che significa? Come posso fare per poter avere il sistema in modalità grafica?

Il problema qui presentato è tipicamente sinonimo di un'errata configurazione del server grafico (ad esempio scheda video o monitor non impostati correttamente...) e lo strano comportamento del monitor è probabilmente imputabile ad X stesso, che prova invano ad avviarsi con diverse risoluzioni/profondità di colore. In questi casi conviene iniziare a **raccogliere il maggior numero possibile di informazioni sulla scheda video** (marca, modello, memoria...) **e sul monitor** (marca, modello, frequenze e risoluzioni supportati); dati alla mano, si può quindi visitare il sito Web della distribuzione utilizzata o del produttore alla ricerca di eventuali driver specifici o di particolari accorgimenti da adottare. A questo punto è possibile autenticarsi nel sistema (facendo per l'appunto il Login) come 'root' e digitare quindi **xf86config** per avviare il programma testuale di configurazione di X (di cui XF86Setup ne è la versione grafica e un po' meno ostica); attenetevi ai valori specificati dal produttore (specialmente per la frequenza del monitor!) e provate prima con risoluzioni basse e crescete man mano. Infine **alcune distribuzioni integrano un proprio tool per la configurazione del server grafico** (sax2 nel caso specifico di SuSE/UnitedLinux).

La documentazione di Linux

Perchè non mi funziona il suono? Ho appena installato Linux ma purtroppo lo scanner, un Epson Perfection 1260, non riesce a funzionare; chi mi può aiutare? Se installo Linux, funzionerà anche la linea ADSL con il mio modem Ericsson? La mia RedHat non mi riconosce il modem Alcatel SpeedTouch USB; qualche idea?

Sono in molti a chiedere aiuto per l'installazione delle periferiche, specialmente modem USB, scanner, schede audio eccetera. Purtroppo la maggior parte dei produttori hardware non rilascia driver per Linux (anche se, lentamente, la situazione sta prendendo una piega diversa) e quindi **ci si deve affidare al lavoro di pochi valorosi (e volontari) Linux-hacker** che scrivono i driver con le loro sante manine. Questo però può ovviamente implicare lunghi tempi di attesa prima che anche Linux supporti questa o quella specifica periferica appena arrivata sul mercato. In primis conviene **visitare il sito Web del produttore** alla ricerca di eventuali driver specifici o di particolari accorgimenti da adottare e quindi ricercare sui siti delle distribuzioni alla ricerca di qualcuna che nell'ultima release abbia inserito il supporto per questo hardware; una ricerca con Google utilizzando come chiavi <**modello della periferica> + linux** vi restituirà sicuramente qualche sito contenente maggiori informazioni e messaggi di altri utenti che prima di voi hanno incontrato questo problema e che, si spera, l'hanno felicemente risolto.. Inoltre per le periferiche USB date un'occhiata anche al sito **http://linux-usb.sf.net**. Ricordatevi, quando inviate un messaggio per chiedere aiuto, di essere il più esaustivi ed essenziali possibile: indicate sempre e marca e modello della periferica ed eventualmente cosa avete già tentato di fare, seppur con scarsi risultati.

Ho installato Mandrake sul mio portatile e funziona tutto a parte il modem integrato PC.Tel.. aiutooo!! Qualcuno potrebbe dirmi come fare per riuscire a far andare il mio Lucent WinModem interno sotto Linux?

Con il termine WinModem (o "soft modems") si indica quella tipologia di modem che, appoggiandosi al driver e quindi al SO, utilizzano il processore stesso della macchina per alcune funzioni. I WinModem risultano essere così meno costosi e pertanto i produttori tendono ad utilizzarli frequentemente, integrandoli nei laptop e inserendoli all'interno di moltissimi PC "assemblati". Se con Windows però i problemi sono limitati, con Linux la situazione assume contorni drammatici. Per lungo tempo infatti non sono stati supportati da Linux e solo **recentemente la situazione è migliorata** grazie al lavoro di alcuni abili programmatori e alla decisione di alcune case (Lucent Technologis in primis) di rilasciare driver anche per il pinguino. Punto di riferimento principale (in lingua Inglese) per tutti i possessori di WinModems è www.linmodems.org; potete inoltre unirvi al gruppo linmodem (http://groups.yahoo.com/group/linmodem) che gestisco e chiedere aiuto, anche in italiano, alla mailing list..

Tra i tanti HOW-TO per Linux sicuramente troverete quello per far funzionare la vostra periferica.

lele - lele@altos.tk

ATTACCHI E DIFESE PER IL PIÙ POPOLARE SPARAMESSAGGI

L'HACKING È ANCHE SU ICQ

Il suo simbolo è ormai sinonimo di messaggi istantanei, ma proprio questa sua grande diffusione ha generato dozzine di programmi maliziosi che ne sfruttano le falle...

Tutti (o quasi) sappiamo che ICQ è un programma che consente l'invio di messaggi in tempo reale ad altri utenti che lo utilizzano. Una volta terminato il download, basta installarlo e registrare un nick o "pseudonimo", per iniziare subito ad utilizzarlo. Registrandovi, **il programma vi assegnerà un UIN (Universal Internet Number), che servirà per identificarvi in rete**; in questo caso, chiunque fosse a conoscenza del vostro numero UIN o Nick, potrà mettersi in contatto con voi. **E proprio qui sta il problema...** Grazie a questa corrispondenza tra numero e persona, un attaccante potrebbe identificare la sua vittima anche se il numero IP cambia a ogni nuovo collegamento.

>> Codici malevoli

Visto il largo utilizzo di ICQ, negli anni sono stati creati degli appositi programmi per hackerarne le funzionalità. Uno dei più famosi è senza dubbio **Infra Red's ICQ Multi War**. Le funzioni di questo programma, apparentemente simpatico ma abbastanza distruttivo, vanno dal semplice **furto delle password** al **bombardamento degli account** con messaggi offensivi. Programmi in grado di proteggerci da questi tipi di attacchi, sono **ICQ Swat** e **Icq Bombsquad**. Questi programmi che ho citato, ma c'è ne sono molti altri, sono in grado di **eliminare in modo molto semplice i messaggi che hanno sommerso il nostro account**. Se siamo a conoscenza del numero UIN o del Nick del nostro molestatore, possiamo attivare la funzione "Ignore" dal programma, che inserisce automaticamente nella lista Ignore i nick sospetti.

>> False identità

Un'altra tecnica utilizzata dai molestatori online è lo " Spoofing " che permette di bombardare un utente di messaggi, facendo sembrare che ogni singolo messaggio provenga da un diverso nick. Altri metodi di protezione li possiamo trovare all'interno di ICQ stesso. Scegliendo dal menu la funzione **Authorization**, possiamo decidere chi informare della nostra vera presenza online. Se la funzione è disattivata, chiunque potrà contattarci o molestarci, ma se l'attiviamo saremo visibili soltanto a chi abbiamo dato l'autorizzazione. Il programma mette a disposizione anche la funzione **Invisible**, che ci renderà invisibili, anche quando siamo realmente connessi alla rete. Una volta attivata questa funzione, non possiamo rimanere sereni, poiché in rete circolano determinati programmi, **creati per smascherare la nostra identità**, inviare messaggi anche senza aver ottenuto l'autorizzazione e vedere se una persona è online indipendentemente dalle impostazioni di visibilità che questa ha impostato sul suo computer.

>> Come proteggersi

Programmi di protezione generale sono **ICQ Watch, Warforge ICQ Protect e ICQ Hacking Utility** Protector. Il primo analizza tutte le connessioni o i tentativi di connessione al nostro ICQ, per evidenziare eventuali tentativi di intrusione; il secondo protegge da eventuali tentativi di "bombardamento" e il terzo racchiude varie funzioni per poter continuare a scambiare messaggini con tranquillità.

Wolf Otakar
www.wolfotakar.com

LINK UTILI

www.red-demon.com/icq.html
Lista di utility e hack per ICQ.

www.darkfall.demon.co.uk/fallen/icq/misc.htm
Utility e tutorial.

www.napolihak.it/pagine/down/icq.php
Una lista più ridotta ma con descrizioni in italiano.

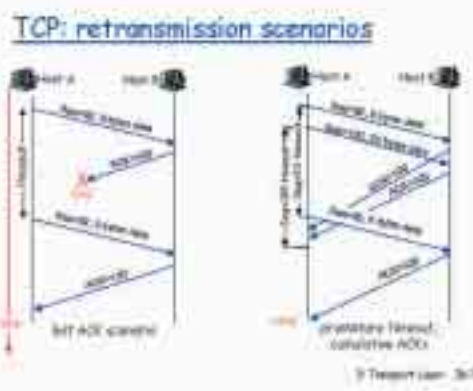
USER DATAGRAM PROTOCOL E TRASMISSION CONTROL PROTOCOL

PACCHETTI SENZA SORPESE

Dopo aver analizzato il livello IP, con le sue caratteristiche, il suo datagram e la sua struttura, è giunto il momento di "salire un gradino" per arrivare al livello superiore, quello per intenderci in cui si ha lo scambio dei pacchetti di trasporto, ed al quale appartengono UDP e TCP.

Prima di entrare nello specifico di questo livello, vogliamo ricordare solo brevissimamente la "torre Internet" formata **alla base dall'hardware**, sopra il quale si impilano i vari livelli costituiti da quello **di interfaccia alla rete** (con lo scambio dei frames), quello di **interconnessioni fra reti o IP** (con lo scambio del datagramma IP), quello di **trasporto, che stiamo per analizzare,** formato da UDP e TCP (con lo scambio dei pacchetti) ed infine l'ultimo detto **livello delle applicazioni** (con lo scambio dei messaggio applicativi).

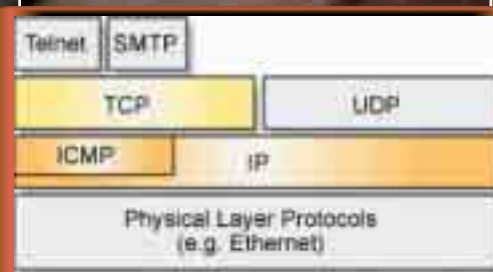
>> Viaggio di un datagramma

Si può dire che ogni datagramma che parte da un host per raggiungerne un altro, sia diretto ad una determinata "macchina". In verità però, è ovvio che quel pacchetto, una volta raggiunta la macchina destinazione, non ha certamente terminato il suo cammino, perché **una volta all'interno del PC dovrà giungere all'applicazione precisa alla quale è destinato**. Com'è quindi possibile ciò? Per semplificare le cose, possiamo dire che l'indirizzo di destinazione di un certo pacchetto, oltre all'IP da raggiungere, che possiamo assimilare alla Via di una città, contiene anche un altro valore detto "porta", assimilabile nel nostro esempio al numero civico al quale si associa senza possibilità di errore uno specifico "nucleo familiare" che rappresenta l'applicazione interessata.

L'UDP permette di associare svariate **protocol port** a un determinato indirizzo IP. Le protocol port non sono altro che dei **punti di ingresso e di uscita dal PC**, ovviamente virtuali. Una volta che un'applicazione chiede accesso ad una determinata porta, nel momento in cui l'ha ottenuto si mette in ascolto su quella porta e tramite questa può ricevere o trasmettere i pacchetti necessari, senza per giunta sapere cosa ci sia al di là della porta stessa. Se per esempio devo spedire un fax tramite il PC io utilizzerò un driver che interfacci il mio computer alla periferica adatta allo scopo; se avessi anche un'altra periferica adatta potrei scollegare la prima ed attaccare la seconda e, nel caso in cui il driver fosse il medesimo, otterrei lo stesso risultato senza che il PC si accorgesse di nulla.

>> Datagrammi UDP

Come IP, anche UDP ha un suo specifico datagramma, anch'esso formato da due parti:

- **Header**: è l'intestazione.
- **Frame data area**: è l'area in cui sono contenuti i dati veri e propri.

L'intestazione in questo caso è assai più semplificata rispetto a quella dell'IP, ed

Torre di internet: livello fisico, livello internet, livello di trasporto e livello applicativo.

è formata solamente da quattro componenti, e per la precisione: **la porta del mittente**, la **porta del destinatario**, la **lunghezza del messaggio** intesa come somma dell'header più l'area dati, e **un checksum** determinante per verificare l'integrità del messaggio stesso. Un'altra analogia con il protocollo IP è "l'inaffidabilità", che può causare la perdita, la duplicazione o l'arrivo errato di un pacchetto.
Un diversità col protocollo IP risiede invece nel calcolo della somma di controllo, formata in questo caso sia dall'intestazione che dall'area dati. Questo campo è opzionale e può quindi essere settato "a zero" nel caso in cui non venga utilizzato. Altra complicazione della somma di controllo sta nel fatto che **non riguarda solamente il datagramma UDP**, ma considera anche altre informazioni, dette aggiuntive, che fanno parte della pseudo-intestazione. Questa è formata dall'indirizzo IP del mittente e del destinatario e da un codice di controllo. Il motivo di questa complicazione è ovvio: essendo un protocollo inaffidabile, come si può stabilire se il pacchetto è giunto alla destinazione corretta senza specificare l'indirizzo IP a cui era indirizzato?

>> Caratteristiche del TCP

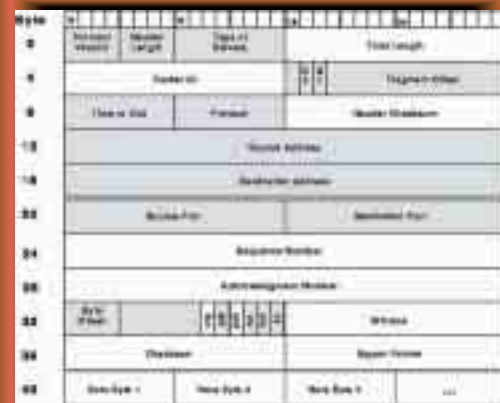
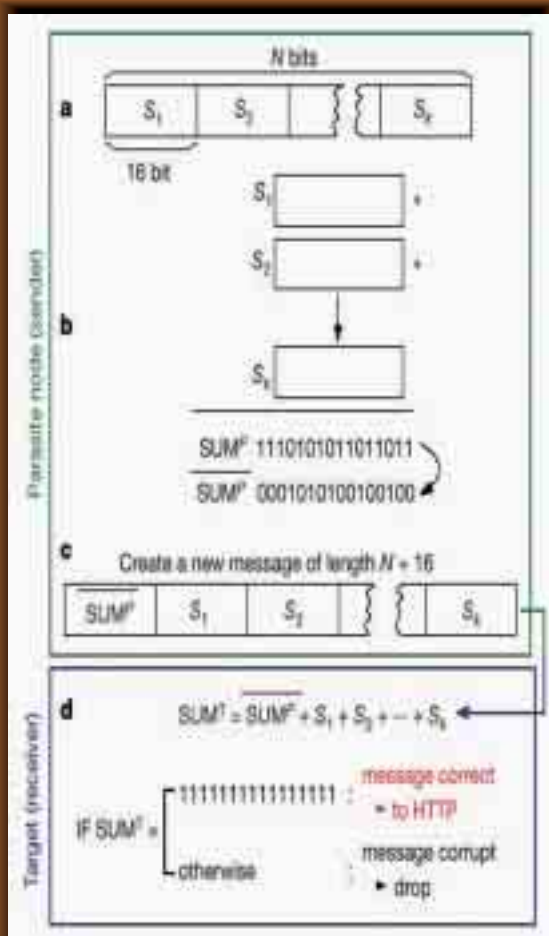
Facente parte dello stesso strato è il TCP. Possiamo tranquillamente dire che esso rappresenta **l'elemento pensante del binomio TCP/IP**, andando a controllare che i dati trasportati da IP siano effettivamente corretti e giungano a destinazione come dovrebbero.
Per capire meglio quali siano i vantaggi di TCP e come mai il binomio TCP/IP sia così stretto e così affidabile, andiamo ad analizzarne le caratteristiche punto per punto:

- TCP è caratterizzato da un **flusso di dati continuo**. Ciò significa che i dati arrivano nell'ordine in cui sono stati spediti, mentre nell'IP avevamo una frammentazione in pacchetti che potevano arrivare in ordine sparso e che inoltre potevano subire un'ulteriore frammentazione durante il cammino nel caso avessero trovato dei "colli di bottiglia" caratterizzati da un soglia di frame fisico minore.

Nel modello a finestre di scorrimento si inviano molti pacchetti prima di ricevere il primo ACK; una volta ricevuto questo si prosegue con l'invio di un'altra serie di pacchetti. Questa tecnica serve per massimizzare la banda e non sprecare risorse.

- TCP usa una **virtual circuit connection**, mentre IP, definendo un solo punto del cammino, non conosce quale strada farà. In verità anche TCP usa un meccanismo a pacchetti, ma definendo i due punti terminali, identifica una **connessione**.
- TCP si può dire che **è "intelligente" ma non è "curioso"**. È intelligente in quanto riesce a ricomporre il flusso dei dati e a passarlo al livello superiore nel miglior modo possibile, ma non è curioso in quanto non si preoccupa mai di sapere cosa stia trasmettendo.
- TCP è una connessione **full duplex**, il che permette di spedire e ricevere dati contemporaneamente.

>> Affidabilità

Abbiamo ripetuto fino alla nausea che IP è inaffidabile, mentre TCP è affidabile; ma **da cosa deriva di fatto questa affidabilità?** L'affidabilità è determinata nel modo più semplice possibile, ovvero nella **conferma, pacchetto per pacchetto, della ricezione dello stesso da parte del destinatario**. Nel momento in cui ha effettuato la spedizione di un pacchetto, TCP si mette in attesa di una "ricevuta di ritorno" da parte del destinatario. Se questa ricevuta arriva nei tempi stabiliti si passa alla spedizione del pacchetto successivo, se non arriva si procede con una nuova spedizione del medesimo pacchetto. Questo sistema prende il nome di **positive acknowledegment with retransmission**.
Come sempre accade non è tutto oro ciò che luccica. Cosa succede se, per un rallentamento della rete, il timer scade e viene inviata un'altra copia dello stesso pacchetto? Succede che magari al ricevente arrivano due copie in giro di poco e ciò potrebbe portare a dei problemi. Inoltre, se setto un timer troppo veloce può darsi che si creino troppi pacchetti duplicati, ma se lo setto troppo lento posso decrementare le prestazioni della rete. Ovviamente per risolvere tutte queste possibili situazioni **sono stati creati appositi algoritmi assai complicati che riescono a ottimizzare le risorse.**

L'header TCP è più complesso di quello UDP, contenendo un numero maggiore di campi e di informazioni Retransmission: nel caso un pacchetto vada perso, allo scadere del suo TTL se non si è ricevuta risposta si provvede al rinvio. La sequenza originale è garantita dai numeri di sequenza dell'intestazione.

Il Tcp Checksum è dato da una pseudointestazione formata dagli indirizzi IP del mittente e de destinatario, dal numero di protocollo e dalla lunghezza dei dati. Poi si aggiungono tanti zeri per renderlo multiplo di 16 e lo divide in parole di 16 bit calcolando la somma a completamento di uno.

Una tecnica fra le svariate utilizzate è quella delle **finestre a scorrimento.** Immaginate di lanciare da un precipizio 5 sassi uno di fila all'altro senza aspettare, come avevamo detto prima, la conferma uno per uno del loro arrivo al suolo. Dopo i primi cinque sassi, nel momento in cui sentiamo il primo "sbong" dell'arrivo, gettiamo il sesto; al secondo "sbong" il settimo e così via. Nel caso si perdesse uno di questi "sbong" significherebbe che quel sassolino (…il pacchetto) non è arrivato e quindi lo rispediremo. Essendo tutti numerati, una volta a destinazione non sarebbe difficile rimetterli in fila anche se fossero giunti in ordine sparso.

>> Dentro a TCP

Per quanto intelligente **anche il nostro TCP ha bisogno di qualche informazione in più per recapitare i dati alla giusta destinazione**. Come nel caso di UDP anche adesso ci vengono incontro le porte di sistema. Al pari delle porte hardware (parallela, seriale, usb…) le porte delle applicazioni sono quelle che danno accesso ad un determinato programma. In principio erano 256 quelle conosciute ed alle quali si associavano responsabilità precise; quelle sopra la 256 erano dinamiche e venivano assegnate di volta in volta. Con il TCP abbiamo introdotto anche il concetto di **connessione**, identificato come una "linea diretta" fra due punti. La connessione è caratterizzata da due estremi, ognuno dei quali a sua volta caratterizzato da due coordinate: l'indirizzo IP e la porta. È chiaro che ogni applicazione può accedere a qualunque porta purché la richiesta provenga da un binomio IP-porta differente.

Come abbiamo visto, TCP ha un sistema abbastanza intuitivo di gestire i dati, ma in verità ci sono due punti importanti da chiarire:

- TCP **ha come unità base il singolo ottetto invece del pacchetto**. Ogni ottetto è numerato ed inviato tramite la finestra a scorrimento, mantenendo però tre riferimenti fondamentali, ovvero: un "registro" in cui scrive gli ottetti arrivati da quelli per cui si aspettano informazioni; un "registro" con gli ottetti spediti e con quelli da spedire; un "registro" con gli ottetti da spedire e con quelli che potranno essere spediti solo dopo lo scorrimento delle finestra in avanti.
- La dimensione della finestra di scorrimento **non è standard**, ma varia e si adatta nel tempo in base alle capacità di ricezione del destinatario. Ciò avviene grazie ad un parametro spedito insieme alla conferma di ricezione che dice se allargare o restringere la finestra stessa.

Analizziamo infine come è formato un segmento TCP. Come sempre esso è fatto da un'intestazione e da un'aera dati. Considerando l'intestazione vediamo che innanzitutto è formata dai numeri di porta del mittente e del destinatario, di 16 bit l'uno; segue il numero di

0	31
Source Port	Destination Port
Length	Checksum
Data	

Il datagramma UDP, semplicissimo, formato solo dalle porte di partenza e di destinazione, dalla lunghezza e dalla somma di controllo.

sequenza dell'ottetto ed il numero di conferma, di 32 bit ciascuno; il primo rappresenta la posizione all'interno dell'area dati che ha quel segmento, il secondo è il numero di conferma che deve arrivare per continuare la ricostruzione. Segue poi il segmento che identifica i dati urgenti, quelli in pratica che devono essere elaborati subito e che non hanno a che fare con la trasmissione in atto precedentemente. Dopo un'area riservata ad usi futuri di 5 bit, abbiamo il campo che indica la posizione dell'area dati nel segmento e 6 bit che identificano 6 distinti segnalatori che indicano al destinatario cosa contiene quel segmento; i sei segnalatori sono: URG, ACK, PSH, RST, SYN, FIN. Il campo seguente indica la capacità della finestra a scorrimento per quel destinatario.

CAT4R4TTA
cat4r4tta@hackerjournal.it

Ucci ucci... sento odor di pacchettucci! (2a parte)

Continuiamo con l'analisi del linsniffer.c, lo sniffer open source per linux di Mike Edulla. Se vi siete persi l'articolo, correte a scaricarvi l'arretrato dalla Secret Zone del nostro sito.

Nel numero precedente abbiamo visto le intestazioni e le variabili struttura che ci serviranno nell'analisi delle funzioni ed abbiamo illustrato i comandi salienti della procedura **openintf che serve ad aprire l'interfaccia di rete in modalità promiscua**. Ritorniamo quindi al **main** che ci fa un po' da guida nell'analisi del codice. La seconda e la terza riga di **main** inizializzano due puntatori precedentemente dichiarati ossia ip e tcp che devono contenere l'header ip e tcp puntando ai campi tcp e ip della variabile struct **ep** di tipo **etherpacket**, anche questa precedentemente dichiarata. Le linee cui mi riferisco sono le seguenti:

```
ip=(struct iphdr *)(((unsigned
                          long)&ep.ip)-2);
tcp=(struct tcphdr *)(((unsigned
                          long)&ep.tcp)-2);
```

In questo caso i reference (cioè gli indirizzi in memoria) delle due variabili ep.ip ed ep.tcp sono passati attraverso un cast ai puntatori ip e tcp. Il cast è una funzione del C che consente di forzare la conversione di tipo per una variabile.
Continuando con la funzione **main** potete notare una serie di funzioni **signal**:

```
signal(SIGHUP, SIG_IGN);
signal(SIGINT, cleanup);
signal(SIGTERM, cleanup);
signal(SIGKILL, cleanup);
signal(SIGQUIT, cleanup);
```

Queste sono utilizzate per la gestione degli interrupt ossia d'eventi esterni al processo in corso che lo interrompono e che possono essere gestiti dal processo stesso attribuendogli un'azione. Il primo parametro in ingresso specifica con una costante il tipo d'interrupt, il secondo può essere anch'esso una costante o una funzione o meglio un puntatore ad una funzione Nel caso specifico vengono installati i gestori dell'interrupt da tastiera (il classico CTRL-c) con la costante SIGINT oppure il segnale di chiusura forzata SIGKILL e altri, che indicano al processo quali eventi devono

generarne la chiusura con il richiamo della funzione **cleanup** che riporto di seguito:

```
void cleanup(int sig)
{
    fprintf(fp, "Exiting...\n");
    close(s);
    fclose(fp);
    exit(0);
}
```

Come potete vedere questa funzione visualizza un messaggio di chiusura, chiude la sessione, chiude il file di log ed esce.

Il file di log

L'ultima parte del **main** è la seguente:

```
if(argc == 2) fp=stdout;
    else fp=fopen(TCPLOG, "at");
    if(fp == NULL) { fprintf(stderr, "cant
                          open log\n");exit(0);}
    clear_victim();
    for(;;)
    {
        read_tcp(s);
        if(victim.active != 0)
print_data(htons(ip->tot_len)-sizeof(ep.ip)-
sizeof(ep.tcp), ep.buff-2);
        fflush(fp);
    }
}
```

Questa parte genera il file di log e lo chiama con il nome stabilito nella label TCPLOG che abbiamo visto nel precedente articolo:

```
#define TCPLOG "test"
```

Naturalmente potete sostituire il nome del file con uno di vostro gradimento.. Qualora l'apertura del file non vada a buon fine, viene restituito un messaggio d'errore. A questo punto linsniffer dopo aver inizializzato l'interfaccia di rete, aver impostato i gestori degli interrupt ed il file di destinazione dei dati è pronto a sniffare. Prima però inizializza la struct victim, che come abbiamo visto nel precedente articolo conterrà i dati della comunicazione "vittima", richiamando la funzione clear_victim, che non vi riporto poiché, come potete vedere anche voi da linsniffer.c, imposta soltanto a zero tutti i campi della struct. Infine avvia la lettura con un ciclo **for** infinito che richiama la funzione che riportiamo di seguito:

```
int read_tcp(int s)
{
    int x;
    while(1)
    {
        x=read(s, (struct etherpacket *)&ep,
sizeof(ep));
        if(x > 1)
        {
            if(filter()==0) continue;
            x=x-54;
            if(x < 1) continue;
            return x;
        }
    }
}
```

Questa funzione riceve in ingresso l'identificativo della sessione precedentemente ottenuto da **openintf** e quindi legge attraverso la funzione **read** i dati provenienti dalla sessione e li inserisce nella struct **ep** ed infine restituisce un intero con la dimensione dei dati sniffati.

Filtri

Tale lettura però non è incondizionata ma opera attraverso un filtro che è costituito dalla funzione **filter()**

```
int filter(void)
{
    int p;
    p=0;
    if(ip->protocol != 6) return 0;
    if(victim.active != 0)
        if(victim.bytes_read > CAPTLEN)
        {
            fprintf(fp, "\n——-
                          [CAPLEN Exceeded]\n");
            clear_victim();
            return 0;
        }
    if(victim.active != 0)
        if(time(NULL) > (victim.start_time +
                                    TIMEOUT))
        {
            fprintf(fp, "\n——- [Timed
                                   Out]\n");
            clear_victim();
            return 0;
        }
    if(ntohs(tcp->dest)==21)  p=1; /* ftp */
    if(ntohs(tcp->dest)==23)  p=1; /* telnet */
    if(ntohs(tcp->dest)==110) p=1; /* pop3 */
```

```
    if(ntohs(tcp->dest)==109) p=1; /* pop2 */
    if(ntohs(tcp->dest)==143) p=1; /* imap2 */
    if(ntohs(tcp->dest)==513) p=1; /* rlogin */
    if(ntohs(tcp->dest)==106) p=1; /* pop
                                     passwd */
    if(ntohs(tcp->dest)==80)  p=1; /* www */
    if(ntohs(tcp->dest)==761) p=1; /*
                             Kerberos "passwd" */
    if(ntohs(tcp->dest)==87)  p=1; /* tty
                                       link */
    if(victim.active == 0)
        if(p == 1)
            if(tcp->syn == 1)
            {
                victim.saddr=ip->saddr;
                victim.daddr=ip->daddr;
                victim.active=1;
                victim.sport=tcp->source;
                victim.dport=tcp->dest;
                victim.bytes_read=0;
                victim.start_time=time(NULL);
                print_header();
            }
    if(tcp->dest != victim.dport) return 0;
    if(tcp->source != victim.sport) return 0;
    if(ip->saddr != victim.saddr) return 0;
    if(ip->daddr != victim.daddr) return 0;
    if(tcp->rst == 1)
    {
        victim.active=0;
        alarm(0);
        fprintf(fp, "\n—- [RST]\n");
        clear_victim();
        return 0;
    }
    if(tcp->fin == 1)
    {
        victim.active=0;
        alarm(0);
        fprintf(fp, "\n—- [FIN]\n");
        clear_victim();
        return 0;
    }
    return 1;
}
```

Questa funzione effettua prima alcuni controlli sulla lunghezza dei dati sniffati per evitare che si superi la quantità di byte definita con CAPTLEN e che non si abbia un time out superiore a quello definito nella label TIMEOUT. Dopo potete notare una serie d'istruzioni if che servono al filtraggio dei pacchetti secondo la porta di provenienza. Qui sono state impostate le porte principali come la porta ftp, telnet, pop3 etc. Voi potete tranquillamente aggiungerne altre a vostro piacimento, qualora vogliate sniffare comunicazioni "particolari". Se ad esempio aggiungo questa linea:

```
if(ntohs(tcp->dest)==53) p=1;
```

posso sniffare anche le comunicazioni sulla porta 53 e così via. A questo punto se la struct con i dati della comunicazione vittima non è attiva viene riempita e viene richiamata al termine la funzione **print_header()** che vedremo nel seguito, se invece la struct è attiva viene effettuato un confronto tra gli estremi dei pacchetti catturati (indirizzo sorgente e destinazione, porta sorgente e destinazione, etc.) e quelli della struct victim; se non c'è corrispondenza la funzione restituisce 0 ed i dati non vengono registrati nel file di log. Qualora poi il filtro verifichi la presenza dei flag FIN (fine connessione) o RST (reset connessione) nel pacchetto TCP, la funzione restituisce 0 ed inizializza sempre a 0 la struct victim.

>> I dati sniffati

Ritornando quindi alla funzione tcp_read, essa restituisce a sua volta a **main** la dimensione del pacchetto sniffato che ha scritto nella struct **ep** di tipo **etherpacket**. La funzione **main** a questo punto si occupa di scrivere sul file di log i dati sniffati attraverso la funzione **print_data**.
Prima di vedere in dettaglio il funzionamento di **print_data** vorrei farvi vedere la funzione **print_header**:

```
int print_header(void)
{
    fprintf(fp, "\n");
    fprintf(fp, "%s => ", hostlookup
                            (ip->saddr));
    fprintf(fp, "%s [%d]\n", hostlookup
            (ip->daddr), ntohs(tcp->dest));
}
```

Questa è la funzione che scrive i dati fondamentali della comunicazione sniffata ossia l'indirizzo origine e destinazione. Richiamando la funzione **hostlookup** fa in modo che vengano scritti gli ip numerici della comunicazione. Vediamo anche la funzione **hostlookup**.

```
char *hostlookup(unsigned long int in)
{
    static char blah[1024];
    struct in_addr i;
    struct hostent *he;

    i.s_addr=in;
    he=gethostbyaddr((char *)&i,
            sizeof(struct in_addr),AF_INET);
    if(he == NULL) strcpy(blah,
                          inet_ntoa(i));
```

```
    else strcpy(blah, he->h_name);
    return blah;
}
```

A questo punto non ci resta che vedere il funzionamento di **print_data** partendo come sempre dalla presentazione del sorgente:

```
int print_data(int datalen, char *data)
{
    int i=0;
    int t=0;

    victim.bytes_read=victim.bytes_read+
                                   datalen;
    for(i=0;i != datalen;i++)
    {
        if(data[i] == 13) { fprintf(fp,
                          "\n"); t=0; }
        if(isprint(data[i])) {fprintf(fp,
                  "%c", data[i]);t++;}
        if(t > 75) {t=0;fprintf(fp, "\n");}
    }
}
```

La funzione riceve in ingresso la lunghezza del buffer da scrivere ed il puntatore all'array dei dati e scrive tutto sul file di log. Con questo abbiamo concluso la lunga descrizione del sorgente di linsniffer. Per utilizzarlo basta compilarlo con la seguente linea di comando

```
gcc linsniffer.c -o linsniffer
```

ed avviarlo lanciando come utente root semplicemente il comando:

```
./linsniffer
```

A questo punto linsniffer dovrebbe catturare e memorizzare tutti i pacchetti che passano attraverso la vostra rete locale e che fanno riferimento alle porte che abbiamo definito nella funzione filter. I dati possono essere letti con qualunque editor di testo aprendo il file di log. Per terminarlo è sufficiente un Ctrl-C.

Alcuni sniffer hanno un'interfaccia grafica a finestre, ma quello descritto in queste pagine è molto più spartano.

Vi consiglio come esercizio di modificare i filtri o la formattazione dei dati per personalizzare il più possibile lo sniffer e per imparare a padroneggiare la programmazione d'applicazioni d'analisi dei pacchetti di cui linsniffer.c è a mio parere un ottimo e educativo esempio.

>> Come cautelarsi

Per concludere vorrei darvi alcune informazioni su **come far fronte all'eventuale installazione di uno sniffer sulla vostra macchina** a vostra insaputa. È possibile verificare attraverso semplici tools se vi siano delle interfacce di rete che operano in modalita promiscua. Uno di questi è **l'ifconfig**, uno strumento utilizzato per configurare i parametri dell'interfaccia di rete. Basta lanciarlo dal prompt dei comandi per scoprire se ci sono "segugi" indesiderati sul vostro sistema. Altri tool che operano come ifconfig potete trovarli in tutte le distribuzioni linux. Inoltre, qualora la vostra interfaccia di rete sia stata impostata in modalità promiscua, al momento della chiusura dell'interfaccia stessa (per esempio quando spegnete la macchina) il sistema dovrebbe segnalarvelo.

A volte l'output di un analizzatore di pacchetti è un po' ostico da leggere, ma facendolo si imparano molte cose sul funzionamento di una rete.

Le funzioni di ifconfig sono solamente in grado di dire se la propria interfaccia di rete è in modalità promiscua, e quindi sta sniffando dati sulla rete locale.
Il vero problema però è capire se qualcun altro, sulla stessa rete, sta utilizzando un computer con scheda di rete in modalità promiscua e uno sniffer, magari puntato proprio sul nostro traffico.
Fortunatamente esistono alcuni applicativi, come NEPED (Network Promiscuous Ethernet Detector), che rivelano le interfacce in modalità promiscua in tutta la sottorete. Il sorgente di NEPED può essere scaricato da www.zone-h.org/files/44/neped.c
NEPED fa anche parte di Trinux, una distribuzione Linux basata su immagine RAM e distribuibile su floppy o CD-ROM che scarica e configura dalla rete una suite di strumenti di sicurezza (port scanner, sniffer, scanner di vulnerabilità, programmi per la costruzione di pacchetti, fingerprinting dell'OS, monitoraggio della rete eccetera...). Le immmagini ISO di Trinux si possono scaricare da http://trinux.sourceforge.net

Roberto "dec0der" Enea
enea@hackerjournal.it